

NISZ Nemzeti Infokommunikációs Szolgáltató Zártkörűen Működő Részvénytársaság

**Hitelesítési rend
a személyazonosító igazolványokhoz kibocsátott
minősített tanúsítványokhoz
(HR-ESZIG)**

Verziószám	1.2
OID	0.2.216.1.200.1100.100.42.3.1.11.1.2
Hatósági azonosító jel	NI-16042701-HR
Hatályba lépés dátuma	2016.05.27
Dokumentum besorolása	nyilvános

© Copyright NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. – Minden jog fenntartva

Változáskövetés

Verzió	Dátum	A változás leírása	Készítette	Ellenőrizte	Jóváhagyta
1.0	2015.11.27	Hatóságnak benyújtott változat nyilvántartásba vételhez	Polysys Kft.	dr. Sandl Judit Kővári Ferenc	Ferencz Attila
1.1	2016.01.07	Hatóság észrevételei alapján módosított változat	Polysys Kft.	dr. Sandl Judit Kővári Ferenc	Ferencz Attila
1.2	2016.04.27	eSZIG tároló elemének BALE tanúsítása miatt módosított változat	Polysys Kft.	dr. Sandl Judit Kővári Ferenc	Ferencz Attila

Tartalomjegyzék

1 BEVEZETÉS	9
1.1 Áttekintés	9
1.2 Dokumentum neve és azonosítása	10
1.2.1 Hitelesítési rendek	10
1.3 PKI közösség	10
1.3.1 Hitelesítő szervezet	10
1.3.2 Regisztrációs Szervezet és Kártyakibocsátó Szervezet	11
1.3.2.1 Regisztrációs Szervezet	11
1.3.2.2 Kártyakibocsátó Szervezet	12
1.3.3 Előfizetők	12
1.3.4 Érintett Felek	12
1.3.5 Egyéb felek	12
1.3.5.1 Postai Szolgáltató	12
1.3.5.2 Felügyeleti Szerv	13
1.4 A tanúsítvány alkalmazhatósága	13
1.4.1 Engedélyezett tanúsítvány használat	13
1.4.2 Tiltott tanúsítvány használat	14
1.5 Szabályzat adminisztráció	14
1.5.1 Szabályzatot karbantartó szerv	14
1.5.2 Kapcsolat	14
1.5.3 HR/HSZSZ alkalmasságának meghatározása	14
1.5.4 HR/HSZSZ jóváhagyásának eljárása	14
1.6 Fogalmak, rövidítések és hivatkozások	15
1.6.1 Fogalmak	15
1.6.2 Rövidítések	20
1.6.3 Hivatkozások	20
1.6.3.1 Jogszabályi hivatkozások	20
1.6.3.2 Szabványok és műszaki-technikai hivatkozások	21
1.6.3.3 Hivatkozott dokumentumok	21
2 KÖZZÉTÉTEL ÉS ADATTÁRAK	23
2.1 Adattárak	23
2.2 Szolgáltatói információ közzététele	23
2.3 A közzététel gyakorisága	23
2.4 Hozzáférés-ellenőrzések	23
3 AZONOSÍTÁS ÉS HITELESÍTÉS	25
3.1 Elnevezések	25
3.1.1 Nevek típusa	25
3.1.2 Nevek jelentése	25
3.1.3 Előfizetők névtelensége és álnév használata	26
3.1.4 Különböző név formák megjelenítési szabályai	26
3.1.5 A nevek egyedisége	26
3.1.6 Márkanév elismerése, hitelesítése és szerepe	26
3.2 Kezdeti azonosítás	26
3.2.1 A magánkulcs birtoklása	26
3.2.2 A szervezeti azonosság hitelesítése	26
3.2.3 A személyazonosság hitelesítése	26
3.2.4 Előfizető nem ellenőrzött adatai	26
3.2.5 Jogosultság ellenőrzése	27
3.2.6 Együttműködési kritériumok	27

3.3	Azonosítás és hitelesítés kulcscsere esetén.....	27
3.3.1	Azonosítás és hitelesítés érvényes tanúsítvány esetén.....	27
3.3.2	Azonosítás és hitelesítés érvénytelen tanúsítvány esetén.....	27
3.4	Azonosítás és hitelesítés visszavonási kérelem esetén.....	27
4	A TANÚSÍTVÁNYOK ÉLETCIKLUSA.....	28
4.1	Tanúsítványigénylés.....	28
4.1.1	Ki nyújthat be tanúsítványigénylést.....	28
4.1.2	Igénylési folyamat és felelősségek.....	28
4.2	Tanúsítványigénylés feldolgozása.....	29
4.2.1	Azonosítási és hitelesítési műveletek.....	29
4.2.2	Tanúsítványigénylés elfogadása vagy visszautasítása.....	29
4.2.3	Tanúsítványigénylés feldolgozás időtartama.....	29
4.3	Tanúsítvány kibocsátás.....	29
4.3.1	Tanúsítványkibocsátás során a Szolgáltató által végzett műveletek.....	29
4.3.2	Előfizető értesítése a tanúsítvány kibocsátásáról.....	30
4.4	Tanúsítvány-elfogadás.....	30
4.4.1	Tanúsítvány Előfizető általi elfogadása.....	30
4.4.2	Tanúsítvány közzététele.....	30
4.4.3	További felek értesítése a tanúsítvány kibocsátásáról.....	30
4.5	A kulcspár és a tanúsítvány használata.....	30
4.5.1	Az Előfizető magánkulcs- és tanúsítvány használata.....	30
4.5.2	Az Érintett Felek nyilvános kulcs- és tanúsítvány használata.....	30
4.6	Tanúsítványok megújítása.....	31
4.6.1	Tanúsítvány megújítás körülményei.....	31
4.6.2	Ki kérelmezhet tanúsítvány megújítást.....	31
4.6.3	Tanúsítvány megújítási kérelmek feldolgozása.....	31
4.6.4	Az Előfizető értesítése a megújított tanúsítvány kibocsátásáról.....	31
4.6.5	Tanúsítvány Előfizető általi elfogadása.....	31
4.6.6	Megújított tanúsítvány közzététele.....	32
4.6.7	További felek értesítése tanúsítvány megújításról.....	32
4.7	Kulcscsere.....	32
4.7.1	Kulcscsere körülményei.....	32
4.7.2	Ki kérelmezhet kulcscserét.....	32
4.7.3	Kulcscsere kérelmek feldolgozása.....	32
4.7.4	Előfizető értesítése az új tanúsítvány kibocsátásáról.....	32
4.7.5	Új tanúsítvány Előfizető általi elfogadása.....	32
4.7.6	Új tanúsítvány közzététele.....	32
4.7.7	További felek értesítése az új tanúsítvány kibocsátásáról.....	32
4.8	Tanúsítvány-módosítás.....	32
4.8.1	Tanúsítvány-módosítás körülményei.....	33
4.8.2	Ki kérelmezhet tanúsítvány-módosítást.....	33
4.8.3	Tanúsítvány-módosítási kérelmek feldolgozása.....	33
4.8.4	Előfizető értesítése az új tanúsítvány kibocsátásáról.....	33
4.8.5	Módosított tanúsítvány Előfizető általi elfogadása.....	33
4.8.6	Módosított tanúsítvány közzététele.....	33
4.8.7	További felek értesítése a módosított tanúsítvány kibocsátásáról.....	33
4.9	Tanúsítvány visszavonás és felfüggesztés.....	33
4.9.1	Visszavonás körülményei.....	33
4.9.2	Ki kezdeményezheti a visszavonást.....	34
4.9.3	Visszavonási kérelemre vonatkozó eljárás.....	34
4.9.4	Kivárási idő visszavonási kérelem esetén.....	34
4.9.5	Visszavonási kérelem feldolgozásának időbelisége.....	34
4.9.6	Visszavonás ellenőrzésének ajánlása az Érintett Felek számára.....	34

4.9.7	CRL kibocsátási gyakoriság.....	34
4.9.8	CRL előállítás és közzététele között leghosszabb idő.....	35
4.9.9	OCSP szolgáltatás biztosítása.....	35
4.9.10	OCSP alapú visszavonás ellenőrzés követelményei.....	35
4.9.11	Visszavonási állapot közlés más formái.....	35
4.9.12	Különleges követelmények a kulcs kompromittálódása esetére.....	35
4.9.13	Felfüggesztés körülményei.....	35
4.9.14	Ki kérelmezhet felfüggesztést.....	35
4.9.15	Felfüggesztésre vonatkozó eljárás.....	35
4.9.16	A felfüggesztés megengedett időtartama.....	36
4.10	Visszavonási állapot szolgáltatások.....	36
4.10.1	Működési jellemzők.....	36
4.10.2	Szolgáltatás rendelkezésre állása.....	36
4.10.3	Opcionális lehetőségek.....	36
4.11	Az előfizetés vége.....	37
4.12	Kulcsletét és visszaállítás.....	37
4.12.1	Kulcsletét és visszaállítás szabályai.....	37
4.12.2	Szimmetrikus rejtjelező kulcs tárolásának és visszaállításának rendje és szabályai.....	37
5	FIZIKAI, ELJÁRÁSBELI ÉS SZEMÉLYZETI BIZTONSÁGI ÓVINTÉZKEDÉSEK.....	38
5.1	Fizikai óvintézkedések.....	38
5.1.1	Telephely elhelyezése és szerkezeti felépítése.....	38
5.1.2	Fizikai hozzáférés.....	38
5.1.3	Áramellátás és légkondicionálás.....	38
5.1.4	Beázás és elárasztás veszélyeztetettség.....	39
5.1.5	Tűz megelőzés és tűzvédelem.....	39
5.1.6	Adathordozók tárolása.....	39
5.1.7	Hulladék kezelése és megsemmisítése.....	39
5.1.8	Fizikailag elkülönítetten őrzött mentési példányok.....	39
5.2	Eljárásbeli előírások.....	40
5.2.1	Bizalmi munkakörök.....	40
5.2.2	Az egyes feladatokhoz szükséges személyzeti létszámok.....	40
5.2.3	Bizalmi munkakörökben elvárt azonosítás és hitelesítés.....	40
5.2.4	Egymást kizáró munkakörök.....	40
5.3	Személyzetre vonatkozó előírások.....	40
5.3.1	Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények.....	41
5.3.2	Biztonsági háttér ellenőrzés eljárásai.....	41
5.3.3	Képzési követelmények.....	41
5.3.4	Továbbképzési gyakoriságok és követelmények.....	41
5.3.5	Munkabeosztás körforgásának gyakorisága és sorrendje.....	41
5.3.6	Felhatalmazás nélküli tevékenységek büntető következményei.....	41
5.3.7	Szerződéses munkavállalókra vonatkozó követelmények.....	42
5.3.8	A személyzet számára biztosított dokumentációk.....	42
5.4	A biztonsági naplózás folyamatai.....	42
5.4.1	Naplózott esemény típusok.....	42
5.4.2	Naplóállomány feldolgozásának gyakorisága.....	42
5.4.3	Naplóállomány megőrzési időtartama.....	42
5.4.4	Naplóállomány védelme.....	42
5.4.5	Naplóállomány mentési folyamatai.....	42
5.4.6	Naplózás gyűjtési rendszere.....	43
5.4.7	Rendellenes eseményeket kiváltó alanyok értesítése.....	43
5.4.8	Sebezhetőség értékelések.....	43
5.5	Adatok archiválása.....	43
5.5.1	A tárolt adatok típusai.....	43

5.5.2	Archívum megőrzési időtartama.....	43
5.5.3	Archívum védelme.....	44
5.5.4	Archívum mentési eljárásai.....	44
5.5.5	Az adatok időbélyegzésére vonatkozó követelmények.....	44
5.5.6	Archívum gyűjtési rendszere.....	44
5.5.7	Archívum hozzáférés és ellenőrzés eljárásai.....	44
5.6	Kulcs átállítás.....	44
5.7	Helyreállítás rendkívüli üzemi helyzetek esetén.....	44
5.7.1	Rendkívüli események és kompromittálódás kezelésének eljárásai.....	45
5.7.2	Sérült számítási erőforrások, szoftverek és/vagy adatok.....	45
5.7.3	Szolgáltató magánkulcsának kompromittálódása esetén követendő eljárás.....	45
5.7.4	Üzletmenet folytonosság helyreállítás katasztrófát követően.....	45
5.8	A szolgáltatási tevékenység megszüntetése.....	46
6	MŰSZAKI BIZTONSÁGI ÓVINTÉZKEDÉSEK.....	47
6.1	Kulcspár előállítás és telepítés.....	47
6.1.1	Kulcspár előállítás.....	47
6.1.2	Magánkulcs eljuttatása a tulajdonoshoz.....	47
6.1.3	Nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz.....	47
6.1.4	A szolgáltatói nyilvános kulcs közzététele.....	47
6.1.5	Kulcs méretek.....	48
6.1.6	A nyilvános kulcs paraméterek előállítása és megfelelőségének ellenőrzése.....	48
6.1.7	A kulcs használat célja (X.509 v3 kulcs használati mezőnek megfelelően).....	48
6.2	Magánkulcs védelme és kriptográfiai modul műszaki szabályozások.....	48
6.2.1	Kriptográfiai modul szabványok és szabályozások.....	48
6.2.2	Több szereplős ("n-ből m") ellenőrzés.....	48
6.2.3	Magánkulcs letét.....	49
6.2.4	Magánkulcs visszaállítása.....	49
6.2.5	Magánkulcs mentése.....	49
6.2.6	Magánkulcs bejuttatása a kriptográfiai modulba.....	49
6.2.7	Magánkulcs kriptográfiai modulban tárolásának módja.....	49
6.2.8	Magánkulcs aktiválásának módja.....	49
6.2.9	Magánkulcs aktív állapotának megszüntetési módja.....	50
6.2.10	Magánkulcs megsemmisítésének módja.....	50
6.2.11	Kriptográfiai modul értékelése.....	50
6.3	Kulcspár gondozás egyéb szempontjai.....	50
6.3.1	Nyilvános kulcs archiválása.....	50
6.3.2	Tanúsítvány érvényességi időszaka és kulcspár felhasználás időtartama	50
6.4	Aktivizáló adatok.....	51
6.4.1	Aktivizáló adatok előállítása és telepítése.....	51
6.4.2	Aktivizáló adatok védelme.....	51
6.4.3	Aktivizáló adatok egyéb szempontjai.....	51
6.5	Informatikai biztonsági óvintézkedések.....	51
6.5.1	Informatikai biztonsági műszaki követelmények meghatározása.....	51
6.5.2	Informatikai biztonsági értékelés.....	52
6.6	Életciklusra vonatkozó műszaki óvintézkedések.....	52
6.6.1	Rendszerfejlesztési óvintézkedések.....	52
6.6.2	Biztonságkezelési óvintézkedések.....	52
6.6.3	Életciklus biztonsági óvintézkedések.....	52
6.7	Hálózatbiztonsági óvintézkedések	52
6.8	Időforrások.....	52
7	TANÚSÍTVÁNY, CRL ÉS OCSP PROFILOK.....	53
7.1	Tanúsítvány profil.....	53
7.1.1	Verziószám.....	53

7.1.2	Tanúsítvány kiterjesztések.....	53
7.1.3	Algoritmus azonosítók.....	53
7.1.4	Név formák.....	53
7.1.5	Név megszorítások.....	53
7.1.6	Hitelesítési rend objektumazonosító.....	53
7.1.7	Szabályzati megszorítások kiterjesztés használata.....	53
7.1.8	Szabályzat minősítők szintaktikája és szemantikája.....	53
7.1.9	A kritikus hitelesítési rendek (Certificate Policies) kiterjesztés feldolgozása.....	54
7.2	CRL profil.....	54
7.2.1	Verziószám.....	54
7.2.2	CRL és CRL bejegyzés kiterjesztések.....	54
7.3	OCSP profil	54
7.3.1	Verziószám.....	54
7.3.2	OCSP kiterjesztések.....	54
8	MEGFELELŐSÉG VIZSGÁLAT ÉS EGYÉB ÉRTÉKELESEK.....	55
8.1	Vizsgálatok gyakorisága és körülményei.....	55
8.2	Auditor azonosítása és képesítése.....	55
8.3	Auditor függetlensége.....	56
8.4	Audit során vizsgált területek.....	56
8.5	Hiányosságok esetén végrehajtandó tevékenységek.....	56
8.6	Eredmény kommunikációja.....	56
9	EGYÉB ÜZLETI ÉS JOGI KÉRDÉSEK.....	57
9.1	Díjak.....	57
9.2	Anyagi felelősség.....	57
9.2.1	Felelősségbiztosítás.....	57
9.2.2	További követelmények.....	57
9.2.3	Felelősségbiztosítás vagy garancia végfelhasználók számára.....	57
9.3	Üzleti információk bizalmassága.....	57
9.3.1	Bizalmasan kezelendő információk köre.....	57
9.3.2	Bizalmasnak nem tekintett információk köre.....	57
9.3.3	Bizalmas információk védelmének felelőssége.....	57
9.4	Személyes adatok védelme.....	58
9.4.1	Adatvédelmi terv.....	58
9.4.2	Bizalmasként kezelendő személyes adatok.....	58
9.4.3	Bizalmasként nem kezelendő személyes adatok.....	58
9.4.4	Személyes adatok védelmének felelőssége.....	58
9.4.5	Hozzájárulás a személyes adatok felhasználásához.....	58
9.4.6	Felfedés hatósági vagy polgári peres eljárás keretében.....	58
9.4.7	Egyéb felfedést eredményező körülmények.....	59
9.5	Szellemi tulajdonjogok.....	59
9.6	Tevékenységért viselt felelősség és helytállás.....	59
9.6.1	Szolgáltató felelőssége és helytállása.....	59
9.6.2	A regisztrációs szervezet felelőssége és helytállása.....	59
9.6.2.1	Regisztrációs Szervezet felelőssége és helytállása.....	59
9.6.2.2	Kártyakibocsátó Szervezet felelőssége és helytállása.....	60
9.6.3	Aláíró felelőssége és helytállása.....	61
9.6.4	Érintett Felek felelőssége és helytállása.....	61
9.6.5	Egyéb felek felelőssége és helytállása.....	61
9.7	Helytállás érvénytelenségi köre.....	61
9.8	Felelősség korlátozása.....	61
9.9	Kártérítések.....	62
9.10	Hatályosság és megszűnés.....	62
9.10.1	Hatályosság.....	62

9.10.2	Megszűnés.....	62
9.10.3	Megszűnés után is hatályban maradó rendelkezések.....	62
9.11	Egyéni hirdetmények és kommunikáció a résztvevőkkel.....	62
9.12	Módosítások.....	62
9.12.1	Módosítás eljárása.....	62
9.12.2	Értesítés módszere és időtartama.....	62
9.12.3	OID megváltozását előidéző körülmények.....	63
9.13	Vitás kérdések rendezése	63
9.14	Irányadó jog.....	63
9.15	Hatályos jognak megfelelés.....	63
9.16	Vegyes rendelkezések.....	63
9.16.1	Teljességi záradék.....	63
9.16.2	Átruházás.....	63
9.16.3	Részleges érvénytelenség.....	63
9.16.4	Igényérvényesítés.....	63
9.16.5	Vis maior.....	63
9.17	Egyéb rendelkezések	64
9.17.1	Hozzáférhetőség a fogyatékkal élő személyek számára.....	64

1 BEVEZETÉS

Jelen dokumentum a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. (továbbiakban mint Kormányzati Hitelesítés Szolgáltató vagy Szolgáltató) Hitelesítési Rendje, amely a tároló elemmel rendelkező személyazonosító igazolvány (továbbiakban: eSZIG) elektronikus aláírás funkciójához szükséges minősített tanúsítvánnyal kapcsolatos szolgáltatásaira vonatkozik (továbbiakban HR-ESZIG).

A Szolgáltató a fenti tárgykörben az alábbi szolgáltatásokat nyújtja:

- a) elektronikus aláírás hitelesítés-szolgáltatás: - az állampolgárok, mint természetes személyek számára elektronikus aláírás célú minősített tanúsítvány kibocsátása, ezen tanúsítványokhoz kapcsolódóan visszavonási és tanúsítvány állapot információk biztosítása;
- b) aláírás-létrehozó eszközön aláírás-létrehozó adat elhelyezése: - elektronikus aláírás létrehozásához használt adatnak (magánkulcsnak) az Aláíró nevében történő előállítás az eSZIG tároló elemén.

Jelen hitelesítési rend a fenti szolgáltatások (továbbiakban Szolgáltatások) keretében kibocsátott minősített tanúsítványok kezelésére (előállítás, kibocsátás, közzététel, megújítás, visszavonás) vonatkozó követelményeket, a tanúsítványok tartalmának és érvényességének ellenőrzési eljárásait és a Szolgáltató működtetésének követelményeit tartalmazza.

A Szolgáltató a Szolgáltatásait a vele szerződéses viszonyban álló állampolgárok (továbbiakban Aláírók) részére nyújtja, de egyes szolgáltatási elemeket hozzáférhetővé tesz az elektronikus aláírások hitelességét ellenőrző Érintett Felek részére is.

1.1 Áttekintés

A hitelesítési rend egy olyan szabálygyűjtemény, amely egy tanúsítvány felhasználhatóságát határozza meg egy közös biztonsági követelményekkel rendelkező közösség és/vagy alkalmazások egy osztálya számára, valamint rögzíti azokat a követelményeket, melyeket a Szolgáltatónak a Szolgáltatások nyújtása során teljesítenie kell.

Jelen hitelesítési rend az {Sz7} RFC 3647 nemzetközi ajánlás alapján készült, felépítésében és tartalmában szigorúan követi annak előírásait.

Jelen hitelesítési rend előírja a természetes személyek számára kibocsátott minősített tanúsítványokkal kapcsolatos, a Szolgáltatások nyújtása során teljesíteni szükséges összes követelményt, melyeket az alábbi nemzetközi szabványok határoznak meg:

- ETSI TS 119 401: General policy requirements for Trust Service Providers {Sz1}
- ETSI TS 119 411-1: Policy and security requirements for Trust Service Providers issuing certificates {Sz2}
- ETSI TS 119 411-2: Policy and security requirements for Trust Service Providers issuing EU qualified certificates {Sz3}
- ETSI TS 119 412-1: Certificate Profiles; Part 1: Overview and common data structures {Sz4}
- ETSI TS 119 412-2: Certificate Profiles; Part 2: Certificate profiles for certificates issued to natural persons {Sz5}
- ETSI TS 119 412-5: Certificate Profiles; Part 5: QCStatements {Sz6}

Ezen követelmények teljesítésének módját, illetve az itt megnevezett eljárások részletes leírását a

NISZ Zrt. "Szolgáltatási szabályzat a személyazonosító igazolványokhoz kibocsátott minősített tanúsítványokhoz" (HSZSZ-ESZIG) dokumentum tartalmazza.

Jelen hitelesítési rendnek megfelelően kibocsátott tanúsítványok az {Sz4} ETSI TS 119-412-1 szabvány 3.1 fejezetében meghatározott "EU minősített tanúsítványok", és tartalmazzák a hitelesítési rend objektum azonosítóját, mely alapján az érintett felek képesek meghatározni az adott tanúsítvány alkalmazhatóságát és megbízhatóságát. Jelen hitelesítési rend v1.2 verziójával kezdődően kibocsátott tanúsítványok biztonságos aláírás-létrehozó eszköz használatát megkövetelő, minősített tanúsítványok.

1.2 Dokumentum neve és azonosítása

Jelen hitelesítési rend teljes neve: NISZ Zrt. "Hitelesítési rend a személyazonosító igazolványokhoz kibocsátott minősített tanúsítványokhoz".

A hitelesítési rend rövid neve: HR-ESZIG.

A hitelesítési rend objektum azonosítója és verziószáma a címlapon található.

A hitelesítési rend hatósági azonosító jele szintén a címlapon található.

A jelen HR-ESZIG hatálya alatt kiadott tanúsítványok kibocsátására és felhasználására vonatkozó részletes szabályokat a HSZSZ-ESZIG szolgáltatási szabályzat tartalmazza.

Jelen HR-ESZIG-nek csak a Szolgáltató elektronikus aláírásával ellátott változata tekinthető hitelesnek.

1.2.1 Hitelesítési rendek

A HR-ESZIG hitelesítési rend megfelel az {Sz3} ETSI TS 119 411-2 szabvány 5.5.1 fejezetében definiált QCP-n-qscd (OID: 0.4.0.194112.1.2) hitelesítési rendnek.

1.3 PKI közösség

Jelen hitelesítési rendben szereplő PKI közösség az alábbi felekből áll:

- Szolgáltató: a jelen hitelesítési rendnek megfelelő tanúsítványokat kibocsátó hitelesítés-szolgáltató, amely a tanúsítványok kibocsátásával és menedzsmentjével kapcsolatos műszaki tevékenységeket végzi;
- Közreműködő Felek: a Szolgáltatóval szerződéses kapcsolatban álló vagy jogszabályban meghatározott, a Szolgáltatások nyújtásában közreműködő felek;
- Végfelhasználók: a tanúsítványt igénylő állampolgár (Aláíró) és a tanúsítvány felhasználásával létrehozott elektronikus aláírásokat fogadó Érintett Felek;
- és Egyéb Felek, azon felek, akik e fenti szerepkörök egyikébe sem sorolhatók.

Azon tevékenységek vonatkozásában, melyeket a Szolgáltató nem maga lát el, Szolgáltató teljes körű felelősséget vállal azért, hogy a Közreműködő Fél tevékenysége során jelen szabályzatban foglalt követelmények teljesülnek.

1.3.1 Hitelesítő szervezet

A hitelesítő szervezet a Szolgáltató központi szervezete, amely a hitelesítő központokból, a szolgáltatás-támogató informatikai rendszerek erőforrásaiból, az ezt körül vevő biztonságos fizikai

környezetből, valamint az üzemeltető és szolgáltatást ellátó személyzetből áll. Feladatai közé tartozik a tanúsítvány igénylések feldolgozása, tanúsítványok kibocsátása, tanúsítványok megújítása, tanúsítványok visszavonása, továbbá a kibocsátott tanúsítványokra vonatkozóan a visszavonási információk szolgáltatása CRL és OCSP formájában.

Jelen hitelesítési rend hatálya alatt Szolgáltató kizárólag az állampolgárok részére, az elektronikus személyazonosító igazolványokhoz (továbbiakban eSZIG) kapcsolódóan bocsát ki tanúsítványokat. Az aláírás létrehozó eszköz az eSZIG tároló elemének elektronikus aláírás funkciót megvalósító része.

Szolgáltató - az email-ben küldött értesítéseket kivéve - az állampolgárokkal közvetlen kapcsolatot nem tart, Aláírók a Regisztrációs Szervezet közreműködésével vehetik igénybe a tanúsítvány kibocsátásra és visszavonás kezelésre irányuló szolgáltatásokat.

Hitelesítési Rend és Szabályozási Csoport

A Hitelesítési Rend és Szabályozási Csoport a Szolgáltató által létrehozott szervezeti egység, amely a hitelesítés szolgáltatással kapcsolatos hitelesítési rendek, szolgáltatási szabályzatok és egyéb szabályzatok elkészítéséért, elfogadásáért, karbantartásáért és adminisztrációjáért felelős.

1.3.2 Regisztrációs Szervezet és Kártyakibocsátó Szervezet

1.3.2.1 Regisztrációs Szervezet

Regisztrációs Szervezet: a {J6} SzigR. 11. § (1) bekezdésben megjelölt *eljáró hatóság*, amely az általa működtetett helyszínekből, valamint az ott dolgozó személyzetből áll. A Regisztrációs Szervezet a Kártyakibocsátó Szervezet által erre a célra kifejlesztett és üzemeltetett informatikai rendszereket és eszközöket használja.

A Regisztrációs Szervezet a Szolgáltatások nyújtásában Közreműködő Fél, feladata a tanúsítványok kibocsátására és visszavonására irányuló igénylésekkel kapcsolatos adminisztratív és operatív tevékenységek ellátása, különösen a tanúsítványok alanyainak azonosítása, adataik rögzítése, ügyfélszolgálati tevékenységek ellátása.

Regisztrációs Irodák

A Regisztrációs Szervezet Regisztrációs Irodákat tart fenn minden olyan helyen, ahol az állampolgár állandó személyazonosító igazolványt igényelhet, azaz az okmányirodákban és kormányablakokban.

Központi Regisztrációs Iroda

A Központi Regisztrációs Iroda az a Regisztrációs Iroda, amely az ügyélforgalom számára nyitva álló helyiségben biztosítja a szolgáltatási szabályzat (HSZSZ-ESZIG) papíralapú példányának elérhetőségét.

Telefonos Ügyfélszolgálat

A Regisztrációs Szervezet Telefonos Ügyfélszolgálatot (Kormányzati Ügyfélvonal - 1818) tart fenn, melynek révén heti hét napban, napi 24 órában biztosítja Aláírók számára a tanúsítvány visszavonásának kezelését, továbbá ellátja a Szolgáltatásokkal kapcsolatos ügyfélszolgálatot.

A Regisztrációs Szervezet felelősségét és kötelezettségeit a 9.6.2.1 fejezet írja le.

1.3.2.2 Kártyakibocsátó Szervezet

Kártyakibocsátó Szervezet: a Szolgáltatóval szerződéses kapcsolatban álló, {J6} SzigR. 4. § szerinti *központi szerv*, az állandó személyazonosító igazolvány (eSZIG) kibocsátója, és az általa működtetett helyszínek és informatikai rendszerek hardver és szoftver összetevőiből, az ezeket körül vevő biztonságos fizikai környezetből, valamint az üzemeltetést ellátó személyzetből áll.

A Kártyakibocsátó Szervezet a Szolgáltatások nyújtásában Közreműködő Fél, feladata az eSZIG gyártásakor vagy utólag az Aláírók kulcspárjainak generálása, visszavonási jelszavak generálása, PUK és PIN kódok előállítása és kártyához rendelése, a Regisztrációs Szervezettől kapott adatokkal a kártya megszemélyesítése (a tároló elemre a polgár {J5} Nytv.-ben meghatározott adatainak felírása), tanúsítványkérelmek eljuttatása Szolgáltatónak, a kiadott tanúsítvány felírása, valamint a visszavonási kérelmek továbbítása Szolgáltatónak.

Az aláírói kulcspárok előállítását végző Kártyakibocsátó Szervezet megfelel a {J8} NekR. által előírt műszaki, technológiai, biztonsági előírásoknak és követelményeknek, valamint teljesíti a biztonságos-aláírás-létrehozó eszköz tanúsítási jelentésében foglalt előírásokat.

A Kártyakibocsátó Szervezet felelősségét és kötelezettségeit a 9.6.2.2 fejezet írja le.

1.3.3 Előfizetők

Előfizető: az állampolgár (Aláíró), aki a tároló elemmel rendelkező személyazonosító igazolványa elektronikus aláírás funkcióját használni kívánja és Szolgáltatási Szerződést köt a Szolgáltatóval a Szolgáltatások igénybe vételére. Aláíró csak a saját nevére szóló tanúsítványt igényelhet, így jelen dokumentum fogalomrendszerében az Előfizető és az Aláíró személye azonos.

Aláíró kizárólagosan birtokolja az eSZIG-et és így az annak tároló elemén levő aláírói kulcspárokat.

Az Aláíró felelősségét és kötelezettségeit a 9.6.3 fejezet írja le.

1.3.4 Érintett Felek

Érintett Fél: a tanúsítványon alapuló elektronikus aláírással ellátott elektronikus dokumentumot fogadó természetes vagy jogi személy, aki/amely az elektronikus aláírássra hagyatkozva jár el a dokumentum hitelességének ellenőrzésekor. Az Érintett Fél nem áll szerződéses viszonyban a Szolgáltatóval.

Az Érintett Félnek az elektronikus aláírás ellenőrzéséhez, a tanúsítvány érvényességének megállapításához minden esetben javasolt igénybe vennie a Szolgáltató visszavonási információt szolgáltató Szolgáltatásait (CRL vagy OCSP).

Az Érintett Felek felelősségét a 9.6.4 fejezet írja le.

1.3.5 Egyéb felek

1.3.5.1 Postai Szolgáltató

A {J6} SzigR. 56. § (4) bekezdésének b) pontja szerinti egyetemes postai szolgáltató (továbbiakban Postai Szolgáltató) a Kártyakibocsátó Szervezettel kötött szerződés alapján végzi az eSZIG, rajta a tároló elemén elhelyezett tanúsítvány és a kapcsolódó elektronikus aláírás létrehozó adat kézbesítését, abban az esetben, ha az állampolgár az eSZIG átvételére a postai

utat jelölte meg.

1.3.5.2 Felügyeleti Szerv

A jogszabályokban megjelölt Felügyeleti Szerv biztosítja a Szolgáltató felügyeletét, ellenőrzi a Szolgáltatások jogszabályi megfelelőségét, ellátja az ezzel kapcsolatos felügyeleti feladatokat. Többek között, figyelemmel kíséri az elektronikus aláírásokkal kapcsolatos technológiai és kriptográfiai algoritmusok fejlődését és határozatba foglalja Szolgáltató szolgáltatásainak nyújtása során használható biztonságos kriptográfiai algoritmusokat, és az azok meghatározott paraméterekkel történő alkalmazására vonatkozó követelményeket; határozatában elrendelheti Szolgáltató számára az aláírói tanúsítvány(ok) visszavonását.

1.4 A tanúsítvány alkalmazhatósága

A HR-ESZIG hatálya alatt kibocsátott tanúsítvány a {J4} Eat. szerinti minősített tanúsítvány, a {J2} 1999/93/EC irányelvvel összhangban, az {Sz4} ETSI TS 119 412-1 szabvány 3.1 fejezetében az „EU minősített tanúsítványra” vonatkozó követelményeknek megfelelően.

A jelen HR-ESZIG szerint kibocsátott tanúsítványok biztonságos aláírás-létrehozó eszköz alkalmazását megkövetelő, minősített tanúsítványok, így a kapcsolódó magánkulccsal együtt minősített elektronikus aláírás létrehozására, illetve ellenőrzésére használhatók.

A minősített elektronikus aláírás joghatását a {J10} polgári perrendtartásról szóló törvény 196. § határozza meg. E szerint a HR-ESZIG hatálya alatt kibocsátott tanúsítvány felhasználásával létrehozott elektronikus aláírással hitelesített elektronikus dokumentum teljes bizonyító erejű magánokirat.

Teszt tanúsítványok

A Szolgáltató - egyrészt saját rendszerének tesztelése céljából, másrészt azért, hogy harmadik felek a Szolgáltatásokat kipróbálhassák - teszt tanúsítványokat is kibocsát. A Szolgáltató semmilyen felelősséget nem vállal a teszt tanúsítványok kibocsátásáért, felhasználásukért, a hozzájuk kapcsolódó szolgáltatások rendelkezésre állásáért.

Szolgáltató az éles szolgáltatást nyújtó gyökér hitelesítő központ hierarchiájában nem bocsát ki teszt tanúsítványt. A teszt tanúsítványok a külön az erre a célra létesített teszt gyökér hitelesítő központ hierarchiájában kerülnek kiadásra.

A teszt tanúsítványok megjelölése olyan módon történik, hogy a tanúsítványban feltüntetett hitelesítési rend objektumazonosító: 0.2.216.1.200.1100.100.42.3.1.999.

A teszt tanúsítványokhoz és azon alapuló elektronikus aláírásokhoz semmilyen joghatás nem kapcsolódik.

1.4.1 Engedélyezett tanúsítvány használat

A kibocsátott tanúsítványokhoz kapcsolódó magánkulcsok kizárólag elektronikus aláírás létrehozására használhatók.

A kibocsátott tanúsítványok, illetve a hozzájuk kapcsolódó nyilvános kulcsok kizárólag elektronikus aláírás érvényesítésére használhatók.

A Szolgáltató területi, pénzügyi, stb. korlátozásokat szabhat a szolgáltatási szabályzatban, melyeket a kibocsátott tanúsítványban fel kell tüntetni.

1.4.2 Tiltott tanúsítvány használat

Tilos a tanúsítványt (illetve a hozzá kapcsolódó kulcspárt) felhasználni titkosításra vagy visszafejtésre, azonosításra, más tanúsítványok aláírására vagy bármilyen hitelesítés-szolgáltatás nyújtásához.

1.5 Szabályzat adminisztráció

1.5.1 Szabályzatot karbantartó szerv

A Szolgáltatónak szervezetén belül Hitelesítési Rend és Szabályozási Csoportot kell működtetnie, amely többek között jelen hitelesítési rend karbantartásáért is felelős.

1.5.2 Kapcsolat

Az ügyfélszolgálati irodák elérhetőségét, nyitva tartását, a Szolgáltatóval való kapcsolattartás módját és az illetékes fogyasztóvédelmi szerv elérhetőségét a szolgáltatási szabályzat tartalmazza.

Szolgáltató adatai:

NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.
Cégjegyzék szám: 01-10-041633
Székhely: 1081 Budapest, Csokonai u. 3.
Levelezési cím: 1389 Budapest, Pf.: 133.
Telefon: +36 1 459 4200
Fax: +36 1 303 1000
Email: eSZIG@hiteles.gov.hu
URL: <http://hiteles.gov.hu>

1.5.3 HR/HSZSZ alkalmasságának meghatározása

A Szolgáltató legalább 24 havonta egyszer megfelelőségértékelő szervezet igénybevételével megfelelőségértékelést végeztet, melynek eredményeit változtatási igényként figyelembe veszi.

A változtatási igényeket a Hitelesítési Rend és Szabályozási Csoport gyűjti, a módosításokat elvégzi, majd ellenőrzésre és jóváhagyásra előterjeszti. Az ellenőrzésre illetve jóváhagyásra a Szolgáltató első szervezete illetve a Szolgáltatásokért felelős vezetője rendelkezik hatáskörrel és felelősséggel.

A jóváhagyás előtt a Szolgáltató megvizsgálja a hitelesítési rend tartalmi és formai megfelelőségét a vonatkozó jogszabályok, előírások és műszaki szabványok tekintetében.

1.5.4 HR/HSZSZ jóváhagyásának eljárása

A hitelesítési rend új verziói mindig új verziószámmal kerülnek nyilvánosságra.

Módosítás esetén a Szolgáltató a HR-ESZIG változtatásokkal egybeszerkesztett új verziójának tervezetét hatósági ellenőrzés és nyilvántartásba vétel céljából átadja, illetve bejelenti az illetékes hatóságnak (Nemzeti Média- és Hírközlési Hatóság), legalább a módosítás életbe lépését megelőzően 30 nappal korábban.

A HR-ESZIG jogszabályoknak való megfelelését a hatóság is ellenőrzi.

A HR-ESZIG új verziója hatályba lépésének feltétele, hogy azt a hatóság nyilvántartásba vegye.

A Szolgáltató a HR-ESZIG új verzióját internetes honlapján közzé teszi. A hatályba lépés napját a dokumentum előlapja tartalmazza.

Az új verzió kötelező érvényű az összes Aláíróra, továbbá az abban foglalt változásokat javasolt figyelembe vennie az összes, a HR-ESZIG előző verzióinak megfelelően kibocsátott tanúsítványokat használó Érintett Félnek.

1.6 Fogalmak, rövidítések és hivatkozások

1.6.1 Fogalmak

Alany: A Szolgáltató által kiadott tanúsítványban azonosított entitás, aki/amely a tanúsítványban szereplő nyilvános kulcsnak megfelelő magánkulcsot birtokolja.

Aláíró: elektronikus aláírást létrehozó természetes személy

Aláírási-ellenőrző adat: olyan egyedi adat (jellemzően kriptográfiai nyilvános kulcs), amelyet az elektronikusan aláírt dokumentumot megismerő személy (vagy eszköz) az elektronikus aláírási ellenőrzésére használ

Aláírási-létrehozó adat: olyan egyedi adat (jellemzően kriptográfiai magánkulcs), amelyet az aláíró az elektronikus aláírási létrehozásához használ

Aláírási-létrehozó eszköz: olyan hardver, illetve szoftver eszköz, melyek segítségével az aláíró az aláírási-létrehozó adatok felhasználásával az elektronikus aláírást létrehozza

Bizalmi Lista: a tagállam által összeállított, fenntartott és közzétett elektronikus lista, amelyben kötelezően szerepelnek a tagállam felelőssége alá tartozó minősített hitelesítés-szolgáltatókra (opcionálisan a nem minősített hitelesítés-szolgáltatók is) valamint e szolgáltatók által nyújtott szolgáltatásokra vonatkozó információk. A Bizalmi Lista automatizált feldolgozásra alkalmas, hitelességét elektronikus aláírási biztosítja.

Biztonságos aláírási-létrehozó eszköz: a {J4} Eat. 1. számú mellékletében foglalt követelményeknek eleget tevő aláírási-létrehozó eszköz

Biztonsági tisztviselő: a bizalmi szolgáltatás biztonságáért, a biztonsági irányelvek és szabályzatok érvényre juttatásáért felelős személy

Biztonságos környezet: olyan fizikai környezet, mely védett illetéktelen hozzáféréstől, és bizonyos mértékig tűz, víz és egyéb katasztrófaeseményektől, egyéb erőszakos behatásoktól

Elektronikus aláírási: elektronikusan aláírt elektronikus dokumentumhoz azonosítás céljából hozzárendelt vagy azzal elválaszthatatlanul összekapcsolt elektronikus adat

Elektronikus aláírási célú tanúsítvány: a hitelesítés-szolgáltató által kibocsátott igazolás, mely az aláírási-ellenőrző adatot (nyilvános kulcsot) egy meghatározott személyhez kapcsolja és igazolja e személy személyazonosságát

Elektronikus aláírás célú minősített tanúsítvány: minősített hitelesítés-szolgáltató által kibocsátott tanúsítvány, amely megfelel a {J4} Eat. 2. számú mellékletében foglalt követelményeknek

Elektronikus aláírás ellenőrzése: az elektronikusan aláírt elektronikus dokumentum aláírás kori, illetve ellenőrzés kori tartalmának összevetése, továbbá az aláíró személyének azonosítása a dokumentumon szereplő, illetve a hitelesítés-szolgáltató által közzétett aláírás-ellenőrző adat, tanúsítvány visszavonási információk, valamint a tanúsítvány felhasználásával

Elektronikus aláírás felhasználása: elektronikus adat elektronikus aláírással történő ellátása, illetve az elektronikus aláírás ellenőrzése

Elektronikus aláírási termék: olyan szoftver vagy hardver, illetve más elektronikus aláírás alkalmazáshoz kapcsolódó összetevő, amely elektronikusan aláírással kapcsolatos szolgáltatások nyújtásához, így különösen elektronikus aláírások, illetőleg időbélyegző létrehozásához vagy érvényesítéséhez használható

Elektronikus azonosítás: a természetes vagy jogi személyt, illetve jogi személyt képviselő természetes személyt egyedileg azonosító, elektronikus személyazonosító adatok felhasználásának folyamata

Elektronikus azonosító eszköz: olyan hardver- és/vagy szoftvereszköz, amely a személyazonosító adatokat tartalmazza, és amelyet online szolgáltatások céljából történő azonosításra használnak

Elektronikus dokumentum: elektronikus eszköz útján értelmezhető adategyüttes

Elektronikus időbélyegző vagy időbélyegző: elektronikusan aláírt elektronikus dokumentumhoz végérvényesen hozzárendelt vagy azzal logikailag összekapcsolt olyan adat, amely igazolja, hogy az elektronikusan aláírt dokumentum az időbélyegző elhelyezésének időpontjában változatlan formában létezett

Előfizető (Aláíró): a természetes személy, aki a Szolgáltatóval érvényes Szolgáltatási Szerződéssel rendelkezik a Szolgáltatások igénybe vételére

Email cím: az Aláíró a Szolgáltatási Szerződés megkötésekor kötelezően meg kell adjon egy email címet. Ez elsődlegesen a Szolgáltató általi kapcsolattartásra szolgál („értesítési email cím”); emellett ez a cím befoglalásra kerül a tanúsítványba is, ha ezt Aláíró kérte. Ha a későbbiekben Aláíró email címe megváltozik (azaz lesz egy új email címe is), és az új címre szeretné megkapni a Szolgáltató értesítéseit, de ezzel együtt a tanúsítványba foglalt email címe nem változott meg (azaz nem szűnt meg, azt továbbra is használja), akkor a két email cím eltér egymástól.

Entitás: a nyilvános kulcsú infrastruktúra (PKI) eleme, pl. egy tanúsítványkiadó, regisztrációs szervezet, végfelhasználó vagy eszköz

eSZIG: A {J5} Nytv. 29. § (1) bekezdésében meghatározott, tároló elemmel ellátott, állandó személyazonosító igazolvány (elektronikus kártya), amely alkalmas az ügyfél elektronikus úton történő közhiteles azonosítására, a polgár kérelmére elektronikus aláírás létrehozására, valamint a polgár a törvényben megjelölt esetekben gyakorolhatja vele a külföldre utazás jogát. A polgár kérelmére tároló eleme tartalmazza az elektronikus aláírás létrehozásához használt adatot és az ahhoz tartozó elektronikus aláírást érvényesítő adatot hitelesítő, elektronikus aláírás célú tanúsítványt.

Érintett fél: az a természetes személy vagy jogi személy, aki/amely az elektronikusan aláírt, és/vagy elektronikusan időbélyegzett dokumentum fogadója, és az adott tanúsítványon alapuló elektronikus aláírásra hagyatkozva jár el az elektronikus aláírás és/vagy az elektronikus időbélyegző hitelességének ellenőrzésekor

Érvényességi lánc: az elektronikus dokumentum vagy annak lenyomata és azon egymáshoz rendelhető információk sorozata (így különösen azon tanúsítványok, tanúsítványokkal kapcsolatos információk, érvényesítési adatok, a tanúsítvány állapotára, visszavonására vonatkozó információk, valamint a tanúsítványt kibocsátó szolgáltató érvényesítési adatára és annak visszavonási állapotára vonatkozó információk), melyek alapján megállapítható, hogy az elektronikus dokumentumon elhelyezett elektronikus aláírás vagy elektronikus időbélyegző, valamint az azokhoz kapcsolódó tanúsítványok az elektronikus aláírás vagy elektronikus időbélyegző elhelyezésének időpontjában érvényes volt

Felhasználó (végfelhasználó): olyan entitás, aki/amely a Szolgáltatások keretében előállított kulcsokat és tanúsítványokat és/vagy időbélyegeket rendeltetésüknek megfelelően használja

Felügyeleti Szerv vagy Hatóság: a {J4} Eat. szerinti az adott tagállamban kijelölt felügyeleti szerv (Magyarországon a Nemzeti Média- és Hírközlési Hatóság), amely a hitelesítés-szolgáltatók felügyeletét végzi, melynek keretében előzetes és utólagos felügyeleti tevékenységek révén ellenőrzi, hogy a szolgáltatók és az általuk nyújtott szolgáltatások eleget tesznek a jogszabályban megállapított követelményeknek

Fokozott biztonságú elektronikus aláírás: olyan elektronikus aláírás, amely

- a) alkalmas az aláíró azonosítására;
- b) egyedülállóan az aláíróhoz köthető;
- c) olyan eszközökkel hozták létre, amelyek kizárólag az aláíró befolyása alatt állnak;
- d) és a dokumentum tartalmához olyan módon kapcsolódik, hogy minden - az aláírás elhelyezését követően a dokumentumon tett - módosítás érzékelhető.

Gyökér hitelesítő központ (ROOT CA, vagy Főtanúsítvány kiadó): az elsőnek létrehozott, fizikailag is működő hitelesítő központ, amely az alája rendelt másodlagos (produktív) hitelesítő központokat hitelesíti

Hitelesítés: olyan elektronikus folyamat, amely lehetővé teszi a természetes vagy jogi személy elektronikus azonosításának vagy az elektronikus adatok eredetének és sértetlenségének az igazolását

Hitelesítési rend (Certificate Policy - CP): olyan szabálygyűjtemény, amelyben a Szolgáltató valamely tanúsítvány felhasználásának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja, illetőleg meghatározott alkalmazások számára

Hitelesítő központ (CA): a Szolgáltató azon egysége, amely a hitelesítés-szolgáltatás magánkulccsal folytatott tevékenységét végzi. Egy hitelesítő központhoz mindig egy magánkulcs tartozik. A hitelesítő központ fizikailag egy telephelyre koncentráltan, védett, biztonságos körülmények között működik.

Időbélyegzés: az a folyamat, melynek során az elektronikus dokumentumhoz elektronikus időbélyegző hozzárendelése történik

Igénylő: az a személy, aki/amely a Szolgáltatóhoz fordul az elektronikus aláírással kapcsolatos szolgáltatások igénybe vétele céljából

Informatikai rendszer: a Szolgáltató által a szolgáltató kulcspár kezeléséhez, az elektronikus aláírás létrehozásához használt adatok előállításához, a tanúsítványok kibocsátásához, a kibocsátott tanúsítványt tartalmazó nyilvántartáshoz, a visszavonási nyilvántartásokhoz és a visszavonás kezelési szolgáltatáshoz, valamint e tevékenységek informatikai védelméhez használt eszközök és termékek

Kompromittálódás: az az eset, amikor a magánkulcs (elektronikus aláírás létrehozásához használt adat vagy elektronikus bélyegző létrehozásához használt adat) használatára arra nem jogosított személy képessé válik vagy azokat megismeri

Kriptográfiai kulcs: olyan kriptográfiai transzformációt vezérlő egyedi jelsorozat, amelynek ismerete a titkosításhoz (rejtjelezéshez) vagy annak visszaállításához, továbbá az elektronikus aláírás előállításához vagy azok érvényesítéséhez szükséges

Kriptográfiai modul (Hardware Security Module - HSM): olyan hardver alapú biztonságos eszköz, amely előállítja, tárolja és védi a kriptográfiai kulcsokat, valamint biztonságos környezetet biztosít a kriptográfiai funkciók végrehajtására

Lenyomat: olyan meghatározott hosszúságú, az elektronikus dokumentumhoz rendelt bitsorozat, amelynek képzése során a használt eljárás (lenyomatképző eljárás) a képzés időpontjában teljesíti a következő feltételeket:

- a képzett lenyomat egyértelműen származtatható az elektronikus dokumentumból;
- a képzett lenyomattól az elvárható biztonsági szinten belül nem lehetséges az elektronikus dokumentum tartalmának meghatározása vagy a tartalomra történő következtetés;
- a képzett lenyomat alapján az elvárható biztonsági szinten belül nem lehetséges olyan elektronikus dokumentum utólagos létrehozatala, melyre alkalmazva a lenyomatképző eljárást, annak eredményeképp az adott lenyomat keletkezik.

Magánkulcs aktiválása: az a folyamat, melynek során a jogosult - különféle azonosító elemek (pl. jelszó, PIN kód megadásával - engedélyezi, hogy az elektronikus aláírást létrehozó eszközön tárolt magánkulcs megkezdje üzemzerű működését. Az aktiválás általában a tanúsítványt igénylő környezetben (dokumentum kezelő, levelező rendszer) történik, és érvényes lehet a visszavonásig (deaktiválásig), illetve egyszeri használatra

Magánkulcs deaktiválása: az a folyamat, melynek során az elektronikus aláírást létrehozó eszközön tárolt magánkulcs üzemzerű működésre megszüntetésre kerül

Megfelelőségértékelő szervezet: a 765/2008/EK rendelet 2. cikkének 13. pontjában meghatározott szervezet, amelyet az említett rendelettel összhangban illetékesnek ismernek el a minősített hitelesítés-szolgáltató és az általa nyújtott minősített szolgáltatások megfelelőségének értékelésére

Minősített hitelesítés-szolgáltató: a {J4} Eat. szabályai szerint nyilvántartásba vett, minősített tanúsítványt a nyilvánosság számára kibocsátó hitelesítés-szolgáltató

Minősített elektronikus aláírás: olyan - fokozott biztonságú - elektronikus aláírás, amelyet az aláíró biztonságos aláírás-létrehozó eszközzel hozott létre, és amelynek hitelesítése céljából minősített tanúsítványt bocsátottak ki

Nyilvános (publikus) kulcsú infrastruktúra (PKI): az elektronikus aláírás, valamint titkosítás létrehozására, érvényesítésére, kezelésére szolgáló, aszimmetrikus kulcspárt alkalmazó infrastruktúra, beleértve a mögöttes intézményrendszert, a különböző hitelesítés-szolgáltatókat és eszközöket is

Produktív hitelesítő központ: a gyökér hitelesítő központ által létrehozott logikailag vagy fizikailag létező hitelesítő központ, amely egy adott alkalmazási, szervezeti, földrajzi, stb. területre ad ki tanúsítványokat

PIN kód: az eSZIG tároló eleméhez rendelt, az elektronikus aláírás funkció használatához szükséges, az aláíró hozzáférési jogosultságát ellenőrző adat. Jelen szabályzat a PIN kód alatt minden esetben az elektronikus aláíráshoz tartozó PIN kódot (nem az állandó személyazonosító igazolványhoz tartozó PIN kódot) érti. Az állampolgár az eSZIG igénylésekor személyesen veszi át a PUK és PIN kódot tartalmazó borítékot. A borítékban átvett PIN kód úgynevezett aktiváló (transzport) PIN kód, amely szükséges az elektronikus aláíráshoz tartozó PIN kód létrehozásához.

PUK kód: az eSZIG tároló eleméhez rendelt, a személyazonosító igazolványhoz tartozó PIN kód és az elektronikus aláíráshoz tartozó PIN sikertelen megadása után használható feloldó adat. A PUK kódot is tartalmazó borítékot az állampolgár személyesen veszi át.

Regisztrációs szervezet: a Szolgáltató és a vele szerződéses alapon vagy jogszabályban meghatározott együttműködő társaságok azon szervezeti egységei, amelyek az állampolgárok adatainak regisztrációját, ellenőrzését, az igénylő személyazonosságának és hitelességének megállapítását, a tanúsítvány kérelmek összeállítását, a hitelesítő szervezethez történő továbbítását, és egyéb azonosítási, tanúsítványmenedzsment és adminisztrációs feladatokat látnak el

Regisztrációs adatok: azon információk, adatok összessége, amelyeket a Szolgáltató a tanúsítványkiadás érdekében az Aláíróról begyűjt

Rendkívüli üzemeltetési helyzet: olyan, a Szolgáltató üzemmenetében zavart okozó rendkívüli helyzet, amikor a Szolgáltató rendes üzemmenetének folytatására ideiglenesen vagy véglegesen nincs lehetőség, beleértve a szolgáltatói magánkulcsok kompromittálódását is, vagy annak közvetlen veszélyét.

Rendszeradminisztrátor: az informatikai rendszer telepítését, konfigurálását, karbantartását végző személy

Rendszerüzemeltető: az informatikai rendszer folyamatos üzemeltetését, mentését és helyreállítását végző személy

Rendszervizsgáló: a szolgáltató naplózott, illetve archivált adatállományait vizsgáló, a szolgáltató által a szabályszerű működés érdekében megvalósított kontroll intézkedések betartásának ellenőrzéséért, a meglévő eljárások folyamatos vizsgálatáért és monitorozásáért felelős személy

Személyazonosító adat: egy természetes vagy jogi személy vagy egy jogi személyt képviselő természetes személy személyazonosságának megállapítását lehetővé tevő adat

Szervezeti elektronikus aláírás: jogi személy, vagy közhiteles nyilvántartásban szereplő jogi személyiség nélküli szervezet által létrehozott elektronikus aláírás; jelen szabályzatban a szervezeti elektronikus aláírás alatt fokozott biztonságú szervezeti elektronikus aláírást kell érteni.

Szolgáltatói kulcspár: a szolgáltatói magánkulcsból és a szolgáltatói nyilvános kulcsból álló, kriptográfiai kulcspár

Szolgáltatói magánkulcs: olyan kriptográfiai magánkulcs, melyet a szolgáltató a saját, elektronikus aláírással kapcsolatos szolgáltatásainak igazolására, így különösen a tanúsítványok

kibocsátásához, visszavonási nyilvántartásokhoz, az időbélyegzéshez, illetve a naplózáshoz használ

Szolgáltatói nyilvános kulcs: olyan kriptográfiai nyilvános kulcs, melyet a szolgáltató magánkulcsának használatával létrehozott elektronikus aláírás vagy elektronikus időbélyegző érvényesítésére használnak

Szolgáltatási szabályzat (Certificate Practice Statement - CPS): a szolgáltató tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazó szabályzat

Tanúsítvány: elektronikus aláírás célú tanúsítvány rövidített megnevezése

Tanúsítvány visszavonási lista (Certificate Revocation List - CRL): valamely okból visszavont vagy felfüggesztett, azaz érvénytelenített tanúsítványok azonosítóit tartalmazó elektronikus lista, melyet a hitelesítés-szolgáltató bocsát ki és hitelesít

Visszavonási jelszó: az elektronikus aláíró tanúsítvány ügyfél kérelmére történő visszavonásához szükséges kód. Az állampolgár a visszavonási jelszót az eSZIG igénylésekor személyesen, lezárt borítékban veszi át.

1.6.2 Rövidítések

BALE		biztonságos aláírás-létrehozó eszköz
CA	Certification Authority	hitelesítő szervezet
CRL	Certification Revocation List	tanúsítvány visszavonási lista
CP	Certificate Policy	hitelesítési rend
CPS	Certificate Practice Statement	hitelesítési szolgáltatási szabályzat
OCSP	Online Certificate Status Protocol	valós idejű tanúsítvány-állapot protokoll
NEK		Nemzeti Egységes Kártyarendszer
NTP	Network Time Protocol	időforrás protokoll
PKI	Public Key Infrastructure	nyilvános kulcsú infrastruktúra
RA	Registration Authority	regisztrációs szervezet

1.6.3 Hivatkozások

1.6.3.1 Jogszabályi hivatkozások

- {J1} 910/2014/EU Európai Parlament és a Tanács rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről (továbbiakban eIDAS)
- {J2} 1999/93/EK Európai Parlament és a Tanács irányelve az elektronikus aláírásra vonatkozó közösségi keretfeltételekről
- {J3} 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól (továbbiakban Ebszt.)

- {J4} 2001. évi XXXV. törvény az elektronikus aláírásról (továbbiakban Eat.)
- {J5} 1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról (Nytv.)
- {J6} 414/2015. (XII.23.) Korm. rendelet a személyazonosító igazolvány kiadása és az egységes arcképmás- és aláírás-felvételezés szabályairól (SzigR.)
- {J7} 2014. évi LXXXIII. törvény az elektronikusártya-kibocsátási keretrendszerről (Nektv.)
- {J8} 53/2015. (IX.24.) BM rendelet az egységes elektronikusártya-kibocsátási keretrendszerről szóló 2014. évi LXXXIII. törvény végrehajtásához szükséges kapcsolódási, műszaki, technológiai, biztonsági előírásokról, követelményekről és a hitelesítési rendről (NekR.)
- {J9} 3/2005. (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről
- {J10} A polgári perrendtartásról szóló 1952. évi III. törvény
- {J11} 2013. évi V. törvény a Polgári Törvénykönyvről

1.6.3.2 Szabványok és műszaki-technikai hivatkozások

- | | | |
|--------|-------------------|---|
| {Sz1} | ETSI TS 119 401 | General policy requirements for Trust Service Providers |
| {Sz2} | ETSI TS 119 411-1 | Policy and security requirements for Trust Service Providers issuing certificates |
| {Sz3} | ETSI TS 119 411-2 | Policy and security requirements for Trust Service Providers issuing EU qualified certificates |
| {Sz4} | ETSI TS 119 412-1 | Certificate Profiles; Part 1: Overview and common data structures |
| {Sz5} | ETSI TS 119 412-2 | Certificate Profiles; Part 2: Certificate profiles for certificates issued to natural persons |
| {Sz6} | ETSI TS 119 412-5 | Certificate Profiles; Part 5: QCStatements |
| {Sz7} | RFC 3647 | Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework |
| {Sz8} | RFC 5280 | Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile |
| {Sz9} | ITU-T X.520 | Information technology - Open Systems Interconnection - The Directory: Selected attribute types |
| {Sz10} | RFC 4514 | Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names |
| {Sz11} | ITU-T X.509 | Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate framework |
| {Sz12} | RFC 6960 | 509 Internet Public Key Infrastructure: Online Certificate Status Protocol - OCSP |

1.6.3.3 Hivatkozott dokumentumok

- | | | |
|------|----------|---------------------------------|
| {D1} | ÁSZF-PKI | Általános Szerződési Feltételek |
|------|----------|---------------------------------|

{D2}	Szolgáltatási Szerződés
{D3}	NISZ Zrt. Szervezeti és Működési Szabályzata
{D4}	NISZ Zrt. Adatvédelmi és adatbiztonsági előírásai
{D5}	NISZ Zrt. PKI szolgáltatások informatikai biztonságpolitikája
{D6}	NISZ Zrt. PKI szolgáltatások biztonsági szabályzata
{D7}	NISZ Zrt. PKI szolgáltatások üzletmenet-folytonossági terve
{D8}	Tanúsítvány profilok a NISZ elektronikus aláírással kapcsolatos szolgáltatásaihoz

2 KÖZZÉTÉTEL ÉS ADATTÁRAK

2.1 Adattárak

A Szolgáltatónak gondoskodnia kell arról, hogy az általa kibocsátott végfelhasználói és szolgáltatói tanúsítványok, a tanúsítványokkal kapcsolatos szabályzatok, a tanúsítványok visszavonási állapotára vonatkozó információk, valamint az egyéb közérdekű szolgáltatói információk az Aláírók és Érintett Felek részére folyamatosan, napi 24 órában, heti hét napban rendelkezésre álljanak. A Szolgáltatónak mindent meg kell tennie annak érdekében, hogy az információk elérhetetlensége ne haladhassa meg a szolgáltatási szabályzatban meghatározott időtartamot.

2.2 Szolgáltatói információ közzététele

A Szolgáltató a szolgáltatói tanúsítványokat, a végfelhasználói és szolgáltatói tanúsítványokkal kapcsolatos szabályzatokat internetes honlapján (<https://hiteles.gov.hu>) teszi közzé, továbbá biztosítja a szolgáltatási szabályzat papíralapú példányának elérhetőségét a Központi Regisztrációs Irodán.

A Szolgáltató a végfelhasználói tanúsítványokat belső tanúsítványtárában tárolja, a kiadott tanúsítványt az Aláíró számára rendelkezésre bocsátja. A szolgáltató a végfelhasználói tanúsítványt internetes honlapján nyilvánosan elérhető, kereshető tanúsítványtárában csak akkor teszi közzé, ha Aláíró a tanúsítvány közzétételéhez hozzájárult.

A Szolgáltató a végfelhasználói és szolgáltatói tanúsítványokkal kapcsolatos visszavonási állapot információkat CRL és OCSP formájában is biztosítja. A visszavonási állapot információk közzétételével kapcsolatos információkat a 4.10 fejezet tartalmazza.

2.3 A közzététel gyakorisága

Szolgáltató a szolgáltatói tanúsítványokat azok kibocsátását követő 24 órán belül teszi közzé.

Szolgáltató a végfelhasználói tanúsítványokat a nyilvánosan kereshető tanúsítványtárban Aláíró hozzájárulása esetén a kibocsátást követő 24 órán belül teszi közzé.

Szolgáltató a tanúsítványokkal kapcsolatos szabályzatokat azok változása esetén közzé teszi legalább 30 nappal a változás hatályba lépését megelőzően.

Szolgáltató a CRL-t legalább 24 óránként frissíti, azaz két egymást követő CRL kibocsátási között idő nem haladja meg a 24 órát. Amennyiben egy tanúsítvány állapota megváltozik, a Szolgáltató a változást követő egy órán belül új CRL-t állít elő és tesz közzé.

Szolgáltató az OCSP szolgáltatása keretében minden OCSP kérésre friss választ állít elő és ad vissza.

2.4 Hozzáférés-ellenőrzések

Szolgáltató olvasás céljára korlátozás nélküli hozzáférést biztosít a szolgáltatói tanúsítványokhoz, a végfelhasználói és szolgáltatói tanúsítványokkal kapcsolatos szabályzatokhoz, a tanúsítványokkal kapcsolatos visszavonási információkhoz.

A végfelhasználói tanúsítványokkal kapcsolatban biztosítja a nyilvános tanúsítványtár kereshetőségét a tanúsítványban tárolt adatok alapján.

Szolgáltató biztonsági intézkedésekkel és eljárási szabályokkal gondoskodik az információkhoz jogosulatlan megváltoztatása, törlése, sérülése és megsemmisülése elleni védelemről.

A kibocsátott tanúsítványokkal kapcsolatos szabályzatoknak csak az elektronikus, aláírással hitelesített formája tekinthető hitelesnek, a dokumentumok nyomtatott változatai semmilyen formában nem tekinthetők hivatalos példánynak vagy hiteles másolatnak.

A szabályzatok papíralapú hiteles példánya megtekinthető a Központi Regisztrációs Irodán.

3 AZONOSÍTÁS ÉS HITELESÍTÉS

3.1 Elnevezések

3.1.1 Nevek típusa

A tanúsítványokban szereplő nevek megadása meg kell, hogy feleljen az {Sz9} ITU-T X.520 ajánlásnak.

A tanúsítvány `Issuer` mezőjében szereplő név legalább az alábbi, {Sz9} ITU-T X.520 szerinti attribútumokat kell, hogy tartalmazza:

- `countryName`;
- `organizationName`;
- `organizationIdentifier`; és
- `commonName`.

Az `Issuer` mező fentiekén túl további attribútumokat is tartalmazhat.

A tanúsítvány `Subject` mezőjében szereplő név kötelezően kell, hogy tartalmazza az alábbi, {Sz9} ITU-T X.520 szerinti attribútumokat:

- `countryName`;
- `givenName` és `surname`;
- `serialNumber`; és
- `commonName`.

A `Subject` mező fentiekén túl további név elemeket is tartalmazhat, azonban nem tartalmazhat álnevet (`pseudonym`).

3.1.2 Nevek jelentése

A tanúsítvány `Issuer` mezőjében szereplő attribútumok jelentése megegyezik az {Sz9} ITU-T X.520 szerintivel. Ezen túl, az `organizationIdentifier` attribútum a Szolgáltató adószámát tartalmazza, tartalma és jelentése megfelel az {Sz4} ETSI TS 119 412-1 5.1.4 fejezetében megadottaknak.

A tanúsítvány `Subject` mezőjében szereplő attribútumok jelentése megegyezik az {Sz9} ITU-T X.520 szerintivel. Ezen túl, az alábbi szabályok érvényesek:

- `countryName`: "HU"
- `givenName`: betű szerint azonosan megegyezik az eSZIG-be foglalt viselt vezetéknévvel, amely egy vagy több családi nevet és "DR." jelzést tartalmazhat, egymástól szóköz karakterrel elválasztva
- `surname`: betű szerint azonosan megegyezik az eSZIG-be foglalt viselt utónévvel, amely egy vagy több keresztnévet és "DR." jelzést tartalmazhat, egymástól szóköz karakterrel elválasztva.
- `serialNumber`: az eSZIG okmányszámát tartalmazza, tartalma és jelentése megfelel az {Sz4} ETSI TS 119 412-1 5.1.3 fejezetében leírtaknak
- `commonName`: a `givenName` és `surname` egymás után fűzése, egymástól szóköz karakterrel elválasztva

3.1.3 Előfizetők névtelensége és álnév használata

Az Aláírók névtelensége és álnév használata nem megengedett.

3.1.4 Különféle név formák megjelenítési szabályai

A tanúsítványba foglalt megkülönböztető nevek (Distinguished Name) ASN.1 szintaxisa az {Sz8} RFC 5280 szerinti, megjelenítési szabályait az {Sz10} RFC 4514 adja meg.

3.1.5 A nevek egyedisége

A Szolgáltatónak biztosítania kell a tanúsítvány `Subject` mezőjébe foglalt megkülönböztető név (Distinguished Name) egyediségét, azaz gondoskodnia kell arról, hogy egy adott megkülönböztető nevet soha nem fog egy másik Aláíróhoz rendelni.

3.1.6 Márkanevek elismerése, hitelesítése és szerepe

Szolgáltató nem foglalja be a tanúsítványba azokat a védjegyeket vagy márkanéveket, melyekkel Aláíró esetleg rendelkezik.

3.2 Kezdeti azonosítás

Az Aláíró személyazonosságának igazolását, a tanúsítványhoz való jogosultságának elbírálását, valamint a tanúsítványba foglalandó adatainak ellenőrzését a Regisztrációs Szervezetnek kell elvégeznie a természetes személy személyes jelenléte útján, az okmányigénylési eljárásrendnek megfelelően.

3.2.1 A magánkulcs birtoklása

Szolgáltatónak meg kell győződnie arról, hogy Aláíró birtokolja a magánkulcsot, melyhez tartozó nyilvános kulcs tanúsítványba foglалását kérelmezi.

3.2.2 A szervezeti azonosság hitelesítése

A tanúsítvány az állampolgárok, mint természetes személyek számára kerül kibocsátásra és magánszemélyi minőségben kerül felhasználásra, így semmilyen szervezeti azonosság nem kerül vizsgálatra és hitelesítésre.

3.2.3 A személyazonosság hitelesítése

A személyazonosság ellenőrzését és hitelesítését a Regisztrációs Szervezet a 3.2 fejezet elején leírt eljárással végzi el.

3.2.4 Előfizető nem ellenőrzött adatai

Szolgáltatónak ellenőriznie kell Aláírónak minden, a tanúsítvány alanyának megkülönböztető nevébe (`Subject`) kerülő adatát.

A tanúsítvány egyéb mezőibe és kiterjesztésébe kerülő adatok tekintetében Szolgáltatónak a

szolgáltatási szabályzatában meg kell jelölnie azokat, melyek nem kerülnek ellenőrzésre.

3.2.5 Jogosultság ellenőrzése

A Regisztrációs Szervezet {J5} Nytv. szabályai szerint ellenőrzi és elbírálja Aláírónak a tanúsítványhoz való jogosultságát.

3.2.6 Együttműködési kritériumok

Szolgáltató a Szolgáltatások nyújtása során nem működik együtt más hitelesítés-szolgáltatókkal.

3.3 Azonosítás és hitelesítés kulcscsere esetén

A Szolgáltató nem nyújt kulcscsere szolgáltatást.

3.3.1 Azonosítás és hitelesítés érvényes tanúsítvány esetén

Nincs kikötés.

3.3.2 Azonosítás és hitelesítés érvénytelen tanúsítvány esetén

Nincs kikötés.

3.4 Azonosítás és hitelesítés visszavonási kérelem esetén

A tanúsítvány visszavonási kérelmet fogadó fél a kérelmező azonosítását és hitelesítését az alábbiak szerint kell végezze:

- a) Aláíró kérelmező esetében: a Regisztrációs Szervezet a 3.2 fejezet elején leírt eljárással vagy a Kormányzati Ügyfélvonal (1818) a visszavonási jelszónak a telefon nyomógombjaival történő megadásával azonosítja és hitelesíti Aláírót;
- b) okmányérvénytelenítést, illetve át nem vett okmányt jelző hatóság esetében: a Szolgáltató PKI, tanúsítvány alapú X.509 azonosítással, valamint a visszavonási kérelmen elhelyezett szervezeti elektronikus aláírás ellenőrzésével hitelesíti a kezdeményezőt.

4 A TANÚSÍTVÁNYOK ÉLETCIKLUSA

A tanúsítványok életciklusának folyamataiban Szolgáltatón kívül a Regisztrációs Szervezet és a Kártyakibocsátó Szervezet működik közre. Szolgáltató teljes körűen felelős a közreműködők tevékenységért, valamint azért, hogy jelen szabályzatban leírt követelmények teljesülnek.

A Szolgáltató felelős minden olyan kárért, amelyet szándékosan vagy gondatlanul bármely természetes vagy jogi személynek okozott, azon kötelezettségei megszegéséből eredően, mely kötelezettségek az esemény időpontjában hatályos, vonatkozó jogszabályban meghatározottak.

A Szolgáltató nem felelős olyan kárért, melyre bizonyítja, hogy az szándékos vagy gondatlan közrehatása nélkül következett be.

Szolgáltató nem felelős a tanúsítvány felhasználására vonatkozó korlátozások be nem tartásából származó károkért.

4.1 Tanúsítványigénylés

4.1.1 Ki nyújthat be tanúsítványigénylést

Tanúsítványigénylést olyan állampolgár nyújthat be, aki tároló elemmel ellátott állandó személyazonosító igazolvány igénylésére a {J5} Nytv. szerint jogosult, vagy érvényes, tároló elemmel ellátott állandó személyazonosító igazolvánnyal már rendelkezik. Az igénylő tanúsítványra jogosultságának elbírálását a Regisztrációs Szervezet végzi.

4.1.2 Igénylési folyamat és felelősségek

A tanúsítványigénylés folyamata röviden a következő:

- tájékoztatás
- regisztráció
- Szolgáltatási Szerződés megkötése
- tanúsítványkérelem előállítása

A folyamatban közvetlenül a Regisztrációs Szervezet, közvetett módon a Kártyakibocsátó Szervezet vesz részt. A Felek a folyamat során PKI autentikációval és titkosítással védett biztonságos csatornán, szervezeti elektronikus aláírással hitelesített üzenetek formájában kommunikálnak egymással. A Felek felelősségeit a 9.6 fejezet tartalmazza.

Tájékoztatás

Igénylőt a Szolgáltatási Szerződés megkötését megelőzően tájékoztatni kell az elektronikus aláírás használati lehetőségeiről, jogszabályi feltételeiről, a szolgáltatási szabályzatról.

Regisztráció

A 3.2 fejezetben leírt azonosítási eljárást követően, az abból származó és közhiteles nyilvántartások alapján ellenőrzött adatokkal kell igénylőnek a tanúsítványba kerülő, illetve a Szolgáltatási Szerződés megkötéséhez szükséges adatait regisztrálni.

Szolgáltatási szerződés megkötése

Szolgáltatónak a Regisztrációs Szervezet közreműködésével kell Aláíróval a Szolgáltatási Szerződést megkötnie. A Szolgáltatási Szerződés tartalmának meg kell felelnie a hatályos jogszabályok előírásainak.

Tanúsítványkérelem előállítása

Regisztrációs Szervezetnek a Kártyakibocsátó Szervezettel együttműködve gondoskodnia kell arról, hogy az eSZIG tároló elemén, az erre a célra szolgáló biztonsági funkciójával generált aláírói kulcspárhoz tartozó tanúsítványkérelem előálljon, és az a Szolgáltatónak továbbításra kerüljön.

4.2 Tanúsítványigénylés feldolgozása

4.2.1 Azonosítási és hitelesítési műveletek

A tanúsítványkérelem igénylőjét (Aláírót) a Regisztrációs Szervezetnek kell azonosítania a 3.2 fejezetben leírt eljárással. Regisztrációs Szervezet csak olyan Aláíró számára állíthat össze tanúsítványkérelmet, akit sikeresen azonosított és aki tanúsítvány igénylésére jogosult.

Szolgáltató csak és kizárólag a Regisztrációs Szervezettől fogadhat tanúsítványkérelmet, melyet PKI autentikációval kell azonosítani, a tanúsítványkérelmek hitelességét az azon elhelyezett szervezeti elektronikus aláírás ellenőrzésével kell elbírálni. Az elektronikus aláírásnak aláírás időpontját hitelesítő időbélyegzőt is kell tartalmaznia.

4.2.2 Tanúsítványigénylés elfogadása vagy visszautasítása

Szolgáltatónak el kell fogadnia a sikeresen azonosított Regisztrációs Szervezettől származó tanúsítványkérelmet, melynek hitelességét az elektronikus aláírás érvényesítésével ellenőrizte.

Szolgáltatónak vissza kell utasítania a tanúsítványkérelmet, ha az nem a Regisztrációs Szervezettől származik, vagy ha a tanúsítványkérelmen elhelyezett elektronikus aláírás nem érvényes.

4.2.3 Tanúsítványigénylés feldolgozás időtartama

Szolgáltatónak a szolgáltatási szabályzatában kell megadnia a tanúsítványkérelem feldolgozására vállalt időtartamot.

4.3 Tanúsítvány kibocsátás

4.3.1 Tanúsítványkibocsátás során a Szolgáltató által végzett műveletek

Szolgáltatónak hosszú távú érvényesítésre alkalmas formára kell kiegészítenie a tanúsítványkérelmen elhelyezett elektronikus aláírást, azt belső nyilvántartásaiban tárolnia kell. Ki kell állítania a tanúsítványt a kérelemből származó adatokkal, azt tanúsításválaszban kell

visszaadnia.

Szolgáltató tanúsításválasza alapján a Kártyakibocsátó Szervezet kell gondoskodjon a kibocsátott tanúsítvány és az ahhoz tartozó szolgáltatói tanúsítványok (tanúsítványlánc) tárolásáról az eSZIG tároló elemének elektronikus aláírás funkciót ellátó részén.

4.3.2 Előfizető értesítése a tanúsítvány kibocsátásáról

Szolgáltatónak a Regisztrációs Szervezet közreműködésével értesítenie kell Aláírót a tanúsítvány kibocsátásáról.

4.4 Tanúsítvány-elfogadás

4.4.1 Tanúsítvány Előfizető általi elfogadása

Aláíró kötelezettsége, hogy az átvett tanúsítványban feltüntetett adatok helyességét mihamarabb ellenőrizze. Amennyiben bármilyen eltérést talál, haladéktalanul intézkednie kell a tanúsítvány visszavonásáról.

4.4.2 Tanúsítvány közzététele

Aláíró hozzájárulása esetén Szolgáltatónak a kibocsátott tanúsítványt közzé kell tennie a nyilvános tanúsítványtárban.

4.4.3 További felek értesítése a tanúsítvány kibocsátásáról

Nincs kikötés.

4.5 A kulcspár és a tanúsítvány használata

4.5.1 Az Előfizető magánkulcs- és tanúsítvány használata

Aláíró csak azt követően használhatja a magánkulcsot és a tanúsítványt, hogy a tanúsítványban foglalt adatok helyességéről meggyőződött.

Aláíró csak az 1.4.1 fejezetben ismertetett célokra és módon használhatja a magánkulcsot és a tanúsítványt.

Előfizetőnek a magánkulcs- és tanúsítvány használata során be kell tartania a 9.6.3 fejezetben ismertetett kötelezettségeit, különösen gondoskodnia kell az aláírás létrehozó eszköz (eSZIG) és az aláírás aktivizáló adat (PIN kód) illetéktelen hozzáférés elleni védelméről.

4.5.2 Az Érintett Felek nyilvános kulcs- és tanúsítvány használata

A jelen hitelesítési rend hatálya alatt kibocsátott tanúsítványon alapuló elektronikus aláírás

elfogadása során szükséges, hogy az Érintett Fél megfelelő körültekintéssel járjon el, melyhez javasolt betartania a szolgáltatási szabályzatban leírt követelményeket, különös tekintettel az alábbiakra:

- a tanúsítványokat csak olyan alkalmazásokban fogadja el, melyek összhangban vannak a a tanúsítvány "kulcshasználat" (KeyUsage) és "kiterjesztett kulcshasználat" (ExtendedKeyUsage) kiterjesztésének tartalmával;
- ellenőrizze a tanúsítvány érvényességét és visszavonási állapotát;
- vegyen figyelembe minden korlátozást, amely a tanúsítványban vagy a tanúsítvány által hivatkozott szabályzatokban szerepel.

4.6 Tanúsítványok megújítása

Az irányadó szabvány ({Sz7} RFC 3647) szerint a tanúsítvány megújítás az a folyamat, amely során Szolgáltató az Aláíró változatlan nyilvános kulcsát és változatlan adatait hitelesíti új érvényességi időtartamra szóló új tanúsítvány kibocsátásával. Ebben az értelemben Szolgáltató nem nyújt tanúsítvány megújítási szolgáltatást, a kulcspárok élettartamára vonatkozó biztonsági megfontolásokból.

A köznapi értelemben vett tanúsítvány megújítást Szolgáltató lehetővé teszi a lejáratot megelőző hatvan napon belül, Aláíró ez irányú kérelmére. Ebben az esetben Aláíró eSZIG-jének tároló elemén - a meglevő kulcspár és tanúsítvány törlésével, illetve felülírásával egyidejűleg - új kulcspár kerül előállításra, és új tanúsítvány kerül kiadásra, melynek érvényességi időszaka a kibocsátás időpontjával kezdődik és attól számított két évig, vagy ha az eSZIG korábban lejár, akkor annak lejáratainak időpontjáig tart.

4.6.1 Tanúsítvány megújítás körülményei

Nincs kikötés.

4.6.2 Ki kérelmezhet tanúsítvány megújítást

Nincs kikötés.

4.6.3 Tanúsítvány megújítási kérelmek feldolgozása

Nincs kikötés.

4.6.4 Az Előfizető értesítése a megújított tanúsítvány kibocsátásáról

Nincs kikötés.

4.6.5 Tanúsítvány Előfizető általi elfogadása

Nincs kikötés.

4.6.6 Megújított tanúsítvány közzététele

Nincs kikötés.

4.6.7 További felek értesítése tanúsítvány megújításról

Nincs kikötés.

4.7 Kulcscsere

A Szolgáltató nem nyújt tanúsítvány kulcscsere szolgáltatást.

4.7.1 Kulcscsere körülményei

Nincs kikötés.

4.7.2 Ki kérelmezhet kulcscserét

Nincs kikötés.

4.7.3 Kulcscsere kérelmek feldolgozása

Nincs kikötés.

4.7.4 Előfizető értesítése az új tanúsítvány kibocsátásáról

Nincs kikötés.

4.7.5 Új tanúsítvány Előfizető általi elfogadása

Nincs kikötés.

4.7.6 Új tanúsítvány közzététele

Nincs kikötés.

4.7.7 További felek értesítése az új tanúsítvány kibocsátásáról

Nincs kikötés.

4.8 Tanúsítvány-módosítás

A Szolgáltató nem nyújt tanúsítvány módosítás szolgáltatást. Aláíró a meglevő tanúsítványában foglalt adatok módosulása esetén új tanúsítványt kell igényeljen.

4.8.1 Tanúsítvány-módosítás körülményei

Nincs kikötés.

4.8.2 Ki kérelmezhet tanúsítvány-módosítást

Nincs kikötés.

4.8.3 Tanúsítvány-módosítási kérelmek feldolgozása

Nincs kikötés.

4.8.4 Előfizető értesítése az új tanúsítvány kibocsátásáról

Nincs kikötés.

4.8.5 Módosított tanúsítvány Előfizető általi elfogadása

Nincs kikötés.

4.8.6 Módosított tanúsítvány közzététele

Nincs kikötés.

4.8.7 További felek értesítése a módosított tanúsítvány kibocsátásáról

Nincs kikötés.

4.9 Tanúsítvány visszavonás és felfüggesztés

A tanúsítvány visszavonása a tanúsítvány érvényességének a tervezett érvényességi idő lejártá előtti megszüntetését jelenti. A visszavonás végleges és visszafordíthatatlan állapot.

A visszavont tanúsítványhoz tartozó magánkulcs használatát azonnal be kell szüntetni. A visszavonási kérelemnek a Szolgáltatóhoz történő megérkezéséig az Aláíró felelős a felmerült károkért. A visszavonási kérelem elfogadásától, a visszavonás tényének közzétételéig a Szolgáltató felelős a felmerülő károkért. Ez alól kivételt képez a bizonyíthatóan csalárd szándékkal történt visszavonás kérés, amely esetben a felmerült károkért a Szolgáltató nem vállal felelősséget. A visszavonás tényének közzététele után az Érintett Fél felelős a felmerülő károkért.

Az Érintett Feleknek ellenőrizniük kell a tanúsítvány visszavonási állapotát a tanúsítványon alapuló elektronikus aláírás elfogadása előtt.

4.9.1 Visszavonás körülményei

Szolgáltatónak a szolgáltatási szabályzatban ismertetnie kell a visszavonáshoz vezető körülményeket.

4.9.2 Ki kezdeményezheti a visszavonást

Visszavonást kezdeményezhet:

- Aláíró;
- az át nem vett okmányokat jelző eljáró hatóság;
- az eSZIG érvénytelenítéséről jogszabály alapján döntő hatóság;
- Szolgáltató.

4.9.3 Visszavonási kérelemre vonatkozó eljárás

Szolgáltatónak ellenőriznie kell a visszavonást kérelmező azonosságát és jogosultságát, valamint ellenőriznie kell a visszavonási kérelemben foglalt adatokat. Ha az ellenőrzések sikeresek, Szolgáltató el kell végezze a tanúsítvány visszavonását és a megváltozott visszavonási állapot információt közzé kell tennie.

A tanúsítvány visszamenőleges visszavonása nem megengedett.

Szolgáltató az egyszer már visszavont tanúsítvány érvényességét nem állíthatja vissza érvényesre.

4.9.4 Kivárási idő visszavonási kérelem esetén

Szolgáltató nem alkalmaz kivárási időt a visszavonási kérelmek teljesítése során.

4.9.5 Visszavonási kérelem feldolgozásának időbelisége

Szolgáltatónak a szolgáltatási szabályzatban meg kell adnia azt a maximális időtartamot, melyen belül a visszavonási kérelmet feldolgozza.

4.9.6 Visszavonás ellenőrzésének ajánlása az Érintett Felek számára

Az Érintett Feleknek a tanúsítvány és az ahhoz felépített tanúsítványlánc minden elemének visszavonási állapotát ellenőriznie kell a tanúsítványból megállapított vagy a 4.10.1 fejezetben megadott elérhetőségekről letöltött CRL vagy megkért OCSP válasz alapján.

4.9.7 CRL kibocsátási gyakoriság

A végfelhasználói tanúsítványokra vonatkozó CRL kibocsátásának gyakorisága: 24 óránként legalább egy CRL. Szolgáltató minden kibocsátáskor törli a CRL-ről azokat a tanúsítványokat, melyek érvényessége a CRL kibocsátásnak időpontjában már lejárt.

A szolgáltatói tanúsítványokhoz kapcsolódó CRL kibocsátásának gyakorisága: 30 naponként legalább egy CRL.

4.9.8 CRL előállítása és közzététele között leghosszabb idő

Szolgáltatónak a szolgáltatási szabályzatban meg kell adnia azt a maximális időtartamot, melyen belül a CRL-t az előállítását követően közzéteszi.

4.9.9 OCSP szolgáltatás biztosítása

Szolgáltatónak a végfelhasználói és szolgáltatói tanúsítványok visszavonási állapotának megállapításához OCSP szolgáltatást is kell nyújtania.

4.9.10 OCSP alapú visszavonás ellenőrzés követelményei

Szolgáltatónak a szolgáltatási szabályzatban meg kell adnia az OCSP alapú visszavonás ellenőrzésével kapcsolatban az Érintett Felek számára fontos figyelmeztetéseket.

4.9.11 Visszavonási állapot közlés más formái

Szolgáltató, a honlapján elérhető nyilvános tanúsítványtárban is közzé teszi a visszavonási állapot információt, tájékoztatási jelleggel. Ez az információ elektronikus aláírás ellenőrzéséhez nem használható fel. Ez a figyelmeztetés a nyilvános tanúsítványtárban is feltüntetésre kerül.

4.9.12 Különleges követelmények a kulcs kompromittálódása esetére

Szolgáltatónak mindent meg kell tennie annak érdekében, hogy a szolgáltatói magánkulcsának kompromittálódása esetén az eseményről az Érintett Feleket értesítse.

A produktív hitelesítő központ magánkulcsának kompromittálódása esetén a Szolgáltatónak képesnek kell lennie az összes érintett végfelhasználói tanúsítvány visszavonására, valamint az adott szolgáltatói tanúsítvány visszavonására. Ebben az esetben a CRL-ben és OCSP válaszokban a tanúsítványok visszavonási ok információt "kulcs kompromittálódás" (keyCompromise) értékre kell állítani.

4.9.13 Felfüggesztés körülményei

Mivel Aláíró a tanúsítvány felfüggesztését a {J6} SzigR. rendelkezései értelmében nem kezdeményezheti, Szolgáltató nem nyújt felfüggesztési szolgáltatást.

4.9.14 Ki kérelmezhet felfüggesztést

Nincs kikötés.

4.9.15 Felfüggesztésre vonatkozó eljárás

Nincs kikötés.

4.9.16 A felfüggesztés megengedett időtartama

Nincs kikötés.

4.10 Visszavonási állapot szolgáltatások

4.10.1 Működési jellemzők

Szolgáltató a végfelhasználói és szolgáltatói tanúsítványokhoz kapcsolódó visszavonási információkat mind CRL, mind OCSP formájában biztosítja.

CRL

A Szolgáltató által kibocsátott CRL megfelel a {Sz8} RFC 5280 szabványnak.

A CRL tartalmaz minden olyan visszavont tanúsítványt, melyek érvényessége a CRL kibocsátásának időpontjában nem járt még le.

Végfelhasználói tanúsítványokra vonatkozó CRL elérhetősége

<http://cca.hiteles.gov.hu/crl/GOVCA-CCA.crl>

Szolgáltatói tanúsítványokra vonatkozó CRL elérhetősége

<http://qca.hiteles.gov.hu/crl/GOVCA-ROOT.crl>

OCSP

A Szolgáltató által biztosított OCSP szolgáltatás megfelel az {Sz12} RFC 6960 szabványnak.

Az OCSP szolgáltatást Szolgáltató az {Sz12} RFC 6960 2.2 fejezetében meghatározott "Authorized Responder" elvnek megfelelően működteti.

Az OCSP válaszadó számára minimum 4 és maximum 21 óránként új, 24 órás érvényességű tanúsítvány kerül kiadásra, annak érdekében, hogy az OCSP választ aláíró tanúsítvány érvényességét ne kelljen ellenőrizni.

Az OCSP szolgáltatás keretében a Szolgáltató biztosítja a visszavonási információt a tanúsítvány lejárát követően is, 10 évig.

Végfelhasználói tanúsítványokra vonatkozó OCSP szolgáltatás elérhetősége

<http://cca.ocsp.hiteles.gov.hu/ocsp-cca>

Szolgáltatói tanúsítványokra vonatkozó OCSP szolgáltatás elérhetősége

<http://qocsp.hiteles.gov.hu/ocsp-root>

4.10.2 Szolgáltatás rendelkezésre állása

A CRL, illetve az OCSP szolgáltatás az év minden napján, napi 24 órában elérhető, 99,9%-os rendelkezésre állással, úgy hogy a kiesés nem lépheti túl esetenként a 3 órás időtartamot.

4.10.3 Opcionális lehetőségek

Nincs kikötés.

4.11 Az előfizetés vége

Aláíró szerződéses viszonya megszűnik a tanúsítvány lejáratával vagy ha a tanúsítvány érvényességének lejáratát megelőzően Aláíró kérésére vagy bármely más okból kifolyólag a tanúsítvány visszavonásra kerül.

4.12 Kulcsletét és visszaállítás

Szolgáltató nem nyújt kulcsletét és visszaállítás szolgáltatást.

4.12.1 Kulcsletét és visszaállítás szabályai

Nincs kikötés.

4.12.2 Szimmetrikus rejtjelező kulcs tárolásának és visszaállításának rendje és szabályai

Nincs kikötés.

5 FIZIKAI, ELJÁRÁSBELI ÉS SZEMÉLYZETI BIZTONSÁGI ÓVINTÉZKEDÉSEK

Szolgáltatónak gondoskodnia kell arról, hogy kellő, az irányadó szabványoknak megfelelő fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések, illetve az ezeket érvényre juttató adminisztratív és irányítási eljárások kerüljenek alkalmazásra.

5.1 Fizikai óvintézkedések

5.1.1 Telephely elhelyezése és szerkezeti felépítése

A Szolgáltató a Szolgáltatások nyújtásában közreműködő informatikai rendszereit fizikai és logikai védelemmel ellátott, legmagasabb védelmi szintet képező objektumában kell elhelyezni és üzemeltetni. A telephely elhelyezése és kialakítása során olyan egymásra épülő és egymást támogató védelmi megoldásokat kell alkalmazni, melyek képesek megakadályozni az illetéktelen hozzáférést és alkalmasak az informatikai rendszerek és Szolgáltató által tárolt bizalmas adatok megővására.

5.1.2 Fizikai hozzáférés

Szolgáltatónak védenie kell a Szolgáltatások nyújtásában közreműködő eszközeit és berendezéseit a jogosulatlan fizikai hozzáféréstől az eszközök manipulálásának megakadályozása érdekében.

Ehhez biztosítani kell, az alábbiakat:

- a gépterembe történő minden belépés naplózásra kerül;
- a gépterembe csak a bizalmi szerepkört betöltő, erre feljogosított munkatárs léphet be, azonosítást követően;
- önálló jogosultsággal nem rendelkező személy csak indokolt és engedélyezett esetben, a szükséges időtartamig tartózkodhat a gépteremben megfelelő jogosultságú kísérő személy állandó felügyelete mellett;
- az eszközök aktivizáló adatai (jelszavak, PIN kódok, stb.) a géptermen belül sem tárolhatók nyílt formában;
- jogosulatlan személy jelenlétében:
 - a bizalmas adatokat tartalmazó adathordozókat fizikailag elzárva tartják;
 - a bejelentkezett terminálok nem maradnak felügyelet nélkül;
 - nem végeznek olyan munkafolyamatot, amely során bizalmas adat felfedésre kerülhet;
- a gépterem elhagyásakor ellenőrzésre kerül:
 - minden eszköz és berendezés megfelelően biztonságos üzemállapotban van;
 - minden terminálon megtörtént a kijelentkezés;
 - a fizikai tároló eszközök megfelelően elzárásra kerültek;
 - a fizikai védelmet biztosító rendszerek és berendezések megfelelően működnek.

5.1.3 Áramellátás és légkondicionálás

Szolgáltató a gépteremben olyan szünetmentes áramellátó rendszert kell biztosítson, amely:

- megfelelő teljesítménnyel rendelkezik a gépterem informatikai és kisegítő létesítményi berendezései áramellátásának biztosítására;
- megvédi az informatikai berendezéseket a külső hálózat feszültség ingadozásai, feszültség kimaradásai és egyéb zavarok ellen;
- tartós áramszünet esetére saját áramellátó berendezés biztosítja - üzemanyag utántöltéssel - tetszőlegesen hosszú időtartamig az áramellátást.

Szolgáltatónak a gépteremben olyan légkondicionáló és levegőszűrő berendezéseket kell alkalmazni, melyek biztosítják az alábbiakat:

- a gépterembe nem juthat be közvetlenül levegő a külső környezetből;
- a gépterem levegőjének tisztasága érdekében a levegőből a por, szennyező anyagok, korrozív anyagok, mérgező vagy gyúlékony anyagok kiszűrésre kerülnek;
- az operátorok biztonságos munkavégzéséhez szükséges mennyiségű oxigén biztosított;
- a levegő nedvességtartalma nem haladja meg az informatikai rendszerek által megkívánt szintet;
- hűtés történik a szükséges üzemi hőmérséklet biztosítására, az eszközök és berendezések túlhevülésének megakadályozására.

5.1.4 Beázás és elárasztás veszélyeztetettség

Szolgáltatónak a géptermet meg kell védenie a beázástól, víz betöréstől és elárasztástól.

5.1.5 Tűzmegelőzés és tűzvédelem

Szolgáltatónak a géptermet füst- és tűzérzékelőkkel kell felszerelni, melyek automatikusan riasztják az illetékes személyzetet. Minden helyiségben jól látható helyen kell elhelyezni a vonatkozó előírásoknak megfelelő típusú és mennyiségű kézi tűzoltó készüléket. A gépteremben automatikus tűzoltó rendszert kell kialakítani, amely emberi egészségre nem veszélyes és nem károsítja az informatikai eszközöket.

5.1.6 Adathordozók tárolása

Szolgáltatónak meg kell védenie valamennyi adathordozóját a jogosulatlan hozzáféréstől, a megsemmisüléstől vagy véletlen rongálódástól.

5.1.7 Hulladék kezelése és megsemmisítése

Szolgáltatónak a környezetvédelmi előírások betartásával kell gondoskodnia feleslegessé vált eszközeinek, adathordozóinak megsemmisítéséről. A felesleges eszközöket és adathordozókat az erre kijelölt munkatárs személyes felügyelete mellett, széleskörűen elfogadott módszerekkel használhatatlanná kell tenni vagy visszaállíthatatlan módon törölni kell.

5.1.8 Fizikailag elkülönítetten őrzött mentési példányok

Szolgáltatónak azt az adatmentést, amiből meghibásodás esetén a teljes szolgáltatás helyreállítható, olyan külső helyszínen kell tárolnia, mely megfelelő fizikai és működési védelemmel rendelkezik. Biztosítani kell a helyszínek között a mentett adatok biztonságos továbbítását.

5.2 Eljárásbeli előírások

Szolgáltatónak gondoskodnia kell arról, hogy informatikai rendszereit biztonságosan, szabályszerűen, a meghibásodás minimális kockázata mellett üzemeltessék. Szolgáltató személyzete a feladatokat olyan eljárásbeli előírások alapján kell végezze, melyek szinkronban vannak a jogszabályi, szabványi és belső biztonsági előírásokkal.

5.2.1 Bizalmi munkakörök

Szolgáltatónak egyértelműen azonosítania kell azokat a munkaköröket, amelyektől a Szolgáltatások biztonsága függ. Ezeket a bizalmi munkaköröket és felelősségeket dokumentálni kell. A jogosultságokat és funkciókat olyan módon kell megosztani az egyes bizalmi munkakörök között, hogy egyedül egyetlen felhasználó se legyen képes a biztonsági védelmi intézkedések megkerülésére.

A bizalmi munkakört betöltő személynek munkaviszonyban kell állnia Szolgáltatóval. Bizalmi munkakörbe a Szolgáltató felső vezetősége kell kinevezze a munkatársakat.

A bizalmi munkakörökön kívül Szolgáltató bizalmi szerepköröket is alkalmazhat. A bizalmi szerepkört betöltő személynek munkaviszonyban kell állnia Szolgáltatóval vagy a Regisztrációs és Kártyakibocsátó Szervezettel.

5.2.2 Az egyes feladatokhoz szükséges személyzeti létszámok

Szolgáltató biztonsági szabályzataiban elő kell írni, hogy csak védett környezetben, kettő, bizalmi munkakört betöltő munkatárs egyidejű fizikai jelenlétében végezhetők el az alábbi műveletek:

- szolgáltatói kulcspár létrehozása;
- szolgáltatói magánkulcs mentése és visszaállítása;
- szolgáltató magánkulcs aktiválása;
- szolgáltatói magánkulcs megsemmisítése.

5.2.3 Bizalmi munkakörökben elvárt azonosítás és hitelesítés

A bizalmi munkaköröket betöltő személyeket azonosítani és hitelesíteni kell, mielőtt a Szolgáltatások nyújtásában érintett, kritikus informatikai rendszerekhez hozzáférnének.

5.2.4 Egymást kizáró munkakörök

A Szolgáltatónak biztosítania kell, hogy a bizalmi munkakörök vonatkozásában:

- a) biztonsági tisztviselő és regisztrációs felelős nem töltheti be a független rendszervizsgálói munkakört;
- b) rendszeradminisztrátor nem töltheti be a biztonsági tisztviselő és a független rendszervizsgálói munkakört;
- c) az informatikai rendszerért általánosan felelős vezető nem láthatja el a biztonsági tisztviselő, illetve a független rendszervizsgáló feladatait;
- d) törekedni kell a bizalmi munkakörök teljes személyi szétválasztására.

5.3 Személyzetre vonatkozó előírások

Szolgáltatónak gondoskodnia kell arról, hogy személyzeti előírásai, a munkatársak alkalmazására vonatkozó gyakorlatai fokozzák és támogatassák a Szolgáltató működésének megbízhatóságát.

5.3.1 Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

Biztosítani kell, hogy bizalmi munkakört csak olyan személyek tölthetnek be, akiknek a bizalmi munkakör betöltéséhez szükséges befolyásmentességét és szakértelmét a Szolgáltató erkölcsi bizonyítvánnyal, szakmai gyakorlattal, végzettséggel és szakképesítéssel igazolni tudja.

5.3.2 Biztonsági háttér ellenőrzés eljárásai

A Szolgáltató vezetői munkakörben, illetve bizalmi munkakörben csak olyan alkalmazottakat foglalkoztathat, akik:

- büntetlen előélettel rendelkeznek és nincs ellenük folyamatban olyan eljárás, ami a büntetlenséget befolyásolhatja (a büntetlen előéletet három hónapnál nem régebbi erkölcsi bizonyítvánnyal kell igazolni);
- nem állnak az elektronikus aláírással kapcsolatos szolgáltatás végzését kizáró foglalkoztatástól eltiltás hatálya alatt;
- a felvételi eljárásban benyújtott önéletrajzban megadott információk valóságát Szolgáltató igazolni tudta.

5.3.3 Képzési követelmények

A bizalmi munkakörökben Szolgáltató olyan személyeket foglalkoztathat, akik az adott munkakör vagy szerepkör ellátásához szükséges mértékben elsajátították:

- a PKI elméletet;
- Szolgáltató informatikai rendszerének sajátosságait és kezelésének módját;
- a szerepkör ellátáshoz szükséges speciális ismereteket;
- Szolgáltató nyilvános és belső szabályzataiban meghatározott folyamatokat és eljárásokat;
- az egyes tevékenységek jogi következményeit;
- az alkalmazandó biztonsági szabályokat.

A Szolgáltató éles informatikai rendszereihez csak a képzést sikeresen záró alkalmazottak kaphatnak hozzáférési jogosultságot.

5.3.4 Továbbképzési gyakoriságok és követelmények

Szolgáltatónak gondoskodnia kell arról, hogy a munkatársak folyamatosan a megfelelő tudással rendelkezzenek, szükség esetén továbbképzést vagy ismétlő jellegű képzést kell tartania.

Legalább évente egyszer továbbképzést kell biztosítani az újonnan ismertté vált sebezhetőségekről, az IT biztonság aktuális gyakorlatáról, a munkatársak saját szakterületét érintően.

5.3.5 Munkabeosztás körforgásának gyakorisága és sorrendje

Nincs kikötés.

5.3.6 Felhatalmazás nélküli tevékenységek büntető következményei

Szolgáltatónak a dolgozókkal kötendő munkaszerződésben szabályoznia kell a dolgozó

felelősségre vonásának lehetőségét a dolgozó által elkövetett mulasztások, vétlen vagy szándékos károkozás esetére.

5.3.7 Szerződéses munkavállalókra vonatkozó követelmények

Szolgáltató bizalmi munkakörben csak munkaviszonyban álló személyt foglalkoztathat.

Az egyéb feladatok ellátására, vállalkozási vagy megbízási szerződésben foglalkoztatott személyeket Szolgáltató csak előzetes biztonsági ellenőrzést követően foglalkoztathatja. Az ellenőrzött személyekkel írásos megállapodást kell kötni, melyben rögzíteni kell az esetleges biztonsági szabályokat és a titoktartásra vonatkozó kikötéseket.

5.3.8 A személyzet számára biztosított dokumentációk

Szolgáltatónak folyamatosan biztosítani kell a személyzet részére a munkakörük ellátásához szükséges dokumentációk és szabályzatok rendelkezésre állását.

5.4 A biztonsági naplózás folyamatai

5.4.1 Naplózott esemény típusok

Szolgáltatónak minden, az informatikai rendszerével és a Szolgáltatások nyújtásával kapcsolatos eseményt naplóznia kell. A naplózott adatállománynak a szolgáltatás nyújtásának teljes folyamatát át kell fognia, és lehetővé tennie, hogy a valós helyzetek megítéléséhez a szükséges mértékben minden, a Szolgáltatásokkal kapcsolatos eseményt rekonstruálni lehessen.

5.4.2 Naplóállomány feldolgozásának gyakorisága

Szolgáltatónak biztosítani kell a naplóállományok rendszeres ellenőrzését és kiértékelését.

5.4.3 Naplóállomány megőrzési időtartama

A naplóállományokat archiválni kell és gondoskodni azok biztonságos megőrzéséről az 5.5.2 fejezetben előírt időtartamig.

5.4.4 Naplóállomány védelme

A naplóállomány minden bejegyzését védeni kell a módosítástól, illetve biztosítani kell, hogy a napló tartalmához csak arra feljogosított személyek férhessenek hozzá.

A naplóállományok kezelését olyan módon kell megoldani, hogy kizárható legyen a napló megsemmisülése, a napló bejegyzések törlése, módosítása, a bejegyzések sorrendjének bármilyen módon történő megváltoztatása.

5.4.5 Naplóállomány mentési folyamatai

A naplóállományokról rendszeres mentést kell készíteni.

5.4.6 Naplózás gyűjtési rendszere

A naplóbejegyzések gyűjtését belső komponenssel kell megoldani. A naplóbejegyzések gyűjtésének meg kell kezdődnie rendszer indításkor és rendszer leállításig folyamatosan működnie kell, és közben biztosítani kell a gyűjtött bejegyzések integritását és rendelkezésre állását, szükség esetén a bizalmasságát is.

A naplóbejegyzések gyűjtési rendszerének működési rendellenessége esetén Szolgáltatónak fel kell függesztenie az érintett területek működését az üzemzavar elhárításáig.

5.4.7 Rendellenes eseményeket kiváltó alanyok értesítése

Nincs kikötés.

5.4.8 Sebezhetőség értékelések

Szolgáltatónak rendszeres időközönként, a naplóállományok és egyéb információk kiértékelésén alapuló sebezhetőség vizsgálatot kell végeznie, mely segítségével feltérképezi a potenciális belső és külső fenyegetéseket, melyek jogosulatlan hozzáférést eredményezhetnek vagy hatással lehetnek a tanúsítvány kibocsátási folyamatra, a tanúsítványban tárolandó adatok megmásítását, módosítását, sérülését vagy megsemmisülését eredményezhetik.

5.5 Adatok archiválása

5.5.1 A tárolt adatok típusai

Szolgáltatónak gondoskodnia kell arról, hogy megőrzésre kerüljön minden olyan információ, amely szükséges ahhoz, hogy egy elektronikus aláírás érvényessége bizonyítható legyen, továbbá amely a Szolgáltató és a rendszereinek megfelelő működését alátámasztja.

Ehhez legalább az alábbi információkat tárolja papír alapon vagy elektronikusan:

- tanúsítványok igénylésével, regisztrációval kapcsolatos minden adat vagy irat, különösen a Szolgáltatási Szerződés, Aláíró által aláírt nyilatkozatok és átvételi elismervények;
- tanúsítványokkal kapcsolatos valamennyi információ a teljes életciklusra vonatkozóan;
- a Postai Szolgáltató által Aláíró számára személyesen kézbesített eSZIG átvételét igazoló elektronikus térítvevények;
- a hitelesítési rend és szolgáltatási szabályzat valamennyi kibocsátott verziója;
- az Általános Szerződési Feltételek valamennyi kibocsátott verziója;
- a Szolgáltató működésével kapcsolatos szerződések, különösen a Közreműködő Felekkel kötött megállapodások;
- valamennyi naplóállomány.

5.5.2 Archívum megőrzési időtartama

Szolgáltató az 5.5.1 fejezetben meghatározott archivált adatokat köteles megőrizni, a tanúsítványokkal kapcsolatos adatok esetében a tanúsítvány érvényességnek lejáratáról számított 10 évig, illetve a tanúsítvánnyal előállított elektronikus aláírással kapcsolatos jogvita jogerős lezárásáig, szabályzatok, szerződések esetében a hatályon kívül helyezés vagy megszűnés utáni

10 évig.

5.5.3 Archívum védelme

Szolgáltatónak biztosítani kell valamennyi archivált adatra azok sértetlenségét és hitelességét, a rendelkezésre állását és a bizalmasságát.

5.5.4 Archívum mentési eljárásai

Szolgáltatónak biztosítani kell az iratok, dokumentumok, elektronikus állományok biztonságos, hosszú távú megőrzését, illetve tárolását.

5.5.5 Az adatok időbélyegzésére vonatkozó követelmények

Valamennyi naplóbejegyzést el kell látni olyan időjellel, melyben legalább egy másodperc pontossággal fel van tüntetve a rendszer által szolgáltatott időpont.

Az elektronikus formában archivált adatokon minősített időbélyeget kell elhelyezni.

Az archivált adatok megőrzése során szükség esetén (pl. algoritmus váltás) gondoskodni kell az elektronikus aláírás hitelességének fenntartásáról.

5.5.6 Archívum gyűjtési rendszere

A naplóállományokat és az egyéb elektronikus keletkezett adatokat a Szolgáltató védett informatikai rendszerén belül kell gyűjteni. A védett informatikai rendszerből történő kizárás során az adatokat minősített időbélyeget tartalmazó elektronikus aláírással kell ellátni.

A papíralapú iratokat a Regisztrációs Irodákból be kell gyűjteni, azokat Szolgáltató dokumentumtárában kell tárolni.

5.5.7 Archívum hozzáférés és ellenőrzés eljárásai

Szolgáltatónak az archivált adatokat meg kell védenie a jogosulatlan hozzáféréstől. A jogosult hozzáféréseket naplózni kell.

5.6 Kulcs átállítás

Szolgáltatónak biztosítani kell, hogy a hitelesítő központok folyamatosan rendelkezzenek a működésükhöz szükséges érvényes kulccsal és tanúsítvánnyal.

Amennyiben új szolgáltatói kulcspár és tanúsítvány előállítása szükséges, Szolgáltatónak ezt olyan módon kell kiviteleznie, hogy az átállítás az Aláírók és Érintett Felek számára a lehető legkisebb kényelmetlenséget jelentse és megfeleljen a vonatkozó jogszabályi és szabványi követelményeknek.

5.7 Helyreállítás rendkívüli üzemi helyzetek esetén

Szolgáltató köteles meghozni minden szükséges intézkedést annak érdekében, hogy rendkívüli

üzemeltetési helyzet, katasztrófa esetén a szolgáltatás kiesésből származó károkat minimalizálja és a Szolgáltatásokat a lehető legrövidebb időn belül helyreállítsa. A rendkívüli üzemeltetési helyzet bekövetkezése esetén a visszavonási nyilvántartások megbízható üzemeltetésének helyreállítása minden más szolgáltatás vagy tevékenység helyreállítását meg kell, hogy előzze.

A visszavonási nyilvántartások, a kibocsátott tanúsítványokat tartalmazó nyilvántartás és a visszavonás kezelési szolgáltatás 3 órát meghaladó kiesése esetén Szolgáltatónak haladéktalanul értesítenie kell a Felügyelet Szervet.

Egyéb incidens esetén - amennyiben az jelentős hatást gyakorol a szolgáltatásra vagy az annak keretében tárolt személyes adatokra -, az elhárítást követően, kell jelenteni az incidenst a Felügyeleti Szervnek.

A bekövetkezett incidens kiértékelése alapján Szolgáltatónak meg kell hoznia a szükséges módosító, javító intézkedéseket, hogy az incidens jövőbeli előfordulását megakadályozza.

5.7.1 Rendkívüli események és kompromittálódás kezelésének eljárásai

Szolgáltatónak rendelkeznie kell üzletmenet folytonossági tervvel.

Rendkívüli üzemeltetési helyzetben Szolgáltatónak dokumentálnia kell az eseményeket, azok körülményeit, az elhárításukra megtett intézkedéseket.

Szolgáltatónak ki kell alakítani és fenntartani egy tartalék CA rendszert, mely a rendkívüli üzemeltetési helyzetben képes a tanúsítványtár és a nyilvános szabályzatok elérhetőségét, a visszavonás kezelési szolgáltatások teljes értékű működését, a CRL-ek közzétételét biztosítani.

A rendkívüli üzemeltetési helyzetben Szolgáltatónak a lehető legrövidebb időn belül tájékoztatást kell közzétennie internetes honlapján, valamint - lehetőség szerint - elektronikus levélben kell értesítenie azokat a személyeket, akiket az esemény érint.

5.7.2 Sérült számítási erőforrások, szoftverek és/vagy adatok

Szolgáltatónak olyan megbízható rendszert kell működtetni, mely a rendszerben bekövetkezett hiba esetén is biztosítja a Szolgáltatások működtetését és elérhetőségét.

5.7.3 Szolgáltató magánkulcsának kompromittálódása esetén követendő eljárás

A Szolgáltató magánkulcsának kompromittálódása esetén haladéktalanul meg kell tenni a szükséges lépéseket:

- visszavonja az összes érintett szolgáltatói tanúsítványt;
- megszünteti az érintett magánkulcs használatát;
- új szolgáltatói kulcspárokat és tanúsítványokat hoz létre;
- értesíti a Felügyeleti Szervet;
- intézkedik valamennyi érintett fél értesítéséről.

5.7.4 Üzletmenet folytonosság helyreállítás katasztrófát követően

Szolgáltatónak rendelkeznie kell tartalék helyszínnel és informatikai rendszerrel, továbbá megtervezett eljárásokkal az áttelepülésre.

5.8 A szolgáltatási tevékenység megszüntetése

Szolgáltatónak rendelkeznie kell a szolgáltatási tevékenység megszüntetésére vonatkozó, aktualizált tervvel.

Szolgáltatónak rendelkeznie kell olyan bankgaranciával, mely fedezi a szolgáltatási tevékenység megszüntetésének költségeit abban az esetben, ha Szolgáltató csődeljárás alá kerül vagy más okból kifolyólag nem képes önmaga fedezni a költségeket.

A szolgáltatási tevékenység megszüntetésére vonatkozó tervnek tartalmaznia kell legalább az alábbiakat:

- Aláírók és Érintett Felek értesítésének módja;
- a Szolgáltatásokban Közreműködő Felek jogosultságainak megvonása;
- a Szolgáltatásokkal kapcsolatos azon kötelezettségeknek átadása egy megbízható félnek, melyek arra vonatkoznak, hogy bizonyítékot szolgáltatassanak a Szolgáltató működésével kapcsolatban - különösen az 5.5.1 fejezetben meghatározott adatoknak a megőrzése az 5.5.2 fejezetben megjelölt időtartamig;
- szolgáltatói magánkulcsok és azok mentései megsemmisítésének módja.

6 MŰSZAKI BIZTONSÁGI ÓVINTÉZKEDÉSEK

6.1 Kulcspár előállítás és telepítés

6.1.1 Kulcspár előállítás

Szolgáltató maga kell előállítsa a tanúsítványok és visszavonási listák aláírására használandó kulcspárokat fizikailag védett környezetben, kriptográfiai modulban (HSM). A kriptográfiai modulnak meg kell felelnie a 6.2.1 fejezet szerinti követelményeknek. A szolgáltató aláírás-létrehozó adatai (magánkulcsai) teljes életciklusuk alatt a kriptográfiai modulban kell maradjanak.

Szolgáltató maga kell előállítsa az OCSP válaszokat aláíró kulcspárokat, fizikailag védett környezetben, HSM modul használata nem követelmény. Az OCSP választ aláíró magánkulcs teljes életciklusa alatt ezen fizikailag védett környezetben kell maradjon.

Aláíró kulcspárját Szolgáltató megbízásából a Kártyakibocsátó Szervezetnek fizikailag védett és biztonságos környezetben, magán az eSZIG-en, annak tároló elemén kell generálnia, melynek BALE tanúsítással kell rendelkeznie. A kulcspár generálás után használatra nem alkalmas, annak aktiválását Aláírónak személyesen kell elvégezni az eSZIG tároló eleméhez rendelt, aktiváló PIN kódjának megadásával.

6.1.2 Magánkulcs eljuttatása a tulajdonoshoz

Amennyiben a tanúsítvány kiadása az új eSZIG okmány igénylésével egyidejűleg történt, a magánkulcs eljuttatása az Aláíróhoz a {J6} SzigR. szerinti eljárásnak megfelelően, a Regisztrációs Szervezetnél, az eSZIG Aláírónak való személyes átadásával történik meg vagy Aláíró választása szerint az eSZIG-et a Postai Szolgáltató kézbesíti személyesen Aláíró vagy meghatalmazottja részére. A postai úton továbbított, át nem vett eSZIG-et Aláíró vagy meghatalmazottja veheti át a kézbesítésre megjelölt cím szerint illetékes járási hivatalban. Ha az eSZIG a kiállításától számított hatvan napon belül nem kerül átvételre, a rajta levő tanúsítványt Szolgáltató az erre vonatkozó hatósági adatszolgáltatás alapján visszavonja.

Amennyiben a tanúsítvány kiadása meglévő (nem újként igényelt) eSZIG-re történt, a magánkulcs eljuttatása Aláíró számára nem szükséges, mivel a kulcspár előállítása Aláíró jelenlétében a már birtokában levő eSZIG tároló elemén, az erre szolgáló biztonsági funkciójának használatával történik, a Regisztrációs Szervezet helyszínén, a Kártyakibocsátó Szervezet informatikai rendszere által.

6.1.3 Nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz

A hitelesítő központ a tanúsítványba foglalandó nyilvános kulcsokat csak az azonosított és feljogosított Kártyakibocsátó Szervezettől, aláírás időpontját hitelesítő időbélyegzőt is tartalmazó szervezeti elektronikus aláírással hitelesített formában fogadhat el.

6.1.4 A szolgáltatói nyilvános kulcs közzététele

Szolgáltatónak biztosítania kell, hogy a szolgáltató nyilvános kulcsa a kicserélésen alapuló

támadás (substitution attack) ellen védett módon legyenek eljuttatva az Érintett Felekhez..

6.1.5 Kulcs méretek

A Szolgáltató a Szolgáltatások nyújtása során - mind a szolgáltatói, mind a végfelhasználói kulcsok tekintetében - , valamint a Szolgáltatások nyújtásában közreműködő feleknek a Felügyeleti Szerv vonatkozó határozatának megfelelő szabványos algoritmusokat, paramétereket és kulchosszakat kell használnia.

6.1.6 A nyilvános kulcs paraméterek előállítása és megfeleltetésének ellenőrzése

A szolgáltatói kulcspárok előállítása a 6.1.1 szerint védett környezetben és tanúsított HSM modulban kell történjen.

A Kártyakibocsátó Szervezet az Aláírók kulcsainak generálását szigorúan védett, biztonságos környezetben és eljárásokkal kell végezze, melynek során be kell tartania a BALE tanúsítási jelentésében foglalt előírásokat is.

6.1.7 A kulcs használat célja (X.509 v3 kulcs használati mezőnek megfelelően)

Szolgáltatónak a tanúsítványokban a `KeyUsage` és `ExtendedKeyUsage` kiterjesztésekben az {Sz11} ITU-T X.509 v3 szabványnak megfelelően kell jeleznie a kulcs használat célját.

6.2 Magánkulcs védelme és kriptográfiai modul műszaki szabályozások

6.2.1 Kriptográfiai modul szabványok és szabályozások

Szolgáltató a szolgáltatói magánkulcsok előállítására, tárolására és használatára csak olyan kriptográfiai modult alkalmazhat, mely rendelkezik a Felügyeleti Szerv által nyilvántartott tanúsító szervezet, vagy az Európai Unió valamely tagállamában nyilvántartásba vett, tanúsításra jogosult szervezet által kiadott igazolással.

Szolgáltató megbízásából a Kártyakibocsátó Szervezetnek az aláírói magánkulcsokat (kulcspárokat) magán az eSZIG tároló elemén (a tároló elem elektronikus aláírással kapcsolatos funkcióját ellátó részén) kell előállítania. Az eSZIG elektronikus aláírással kapcsolatos funkcióját ellátó részének rendelkeznie kell a Felügyeleti Szerv által nyilvántartott tanúsító szervezet, vagy az Európai Unió valamely tagállamában nyilvántartásba vett, tanúsításra jogosult szervezet által kiadott igazolással a biztonságos aláírás-létrehozó eszköz követelményeinek való megfelelésről.

6.2.2 Több szereplős ("n-ből m") ellenőrzés

Szolgáltató a hitelesítő központokban alkalmazza a több szereplős "n-ből m" ellenőrzést a gyökér hitelesítő központ kulcsgondozási funkcióinak aktivizálásánál.

6.2.3 Magánkulcs letét

Szolgáltató a hitelesítő központok magánkulcsait nem teszi letétbe semmilyen célból.

Szolgáltató nem nyújt az Aláírók számára magánkulcs letét szolgáltatást.

6.2.4 Magánkulcs visszaállítása

Szolgáltatói hitelesítő központok magánkulcsai biztonsági okokból mentésre kerülnek. A mentés titkosított formában, speciális eszközök alkalmazásával történik. Szolgáltató a hitelesítő központok magánkulcsait rendkívüli üzemi helyzetek esetén a titkosított mentésből visszaállíthatja, ugyanolyan fizikai, biztonsági óvintézkedések és eljárási szabályok betartásával, mint ahogy a magánkulcs előállítása eredetileg történt.

A Szolgáltató megbízásából eljáró Regisztrációs Szervezet és Kártyakibocsátó Szervezet az Aláíró magánkulcsát semmilyen formában nem menti, nem tárolja.

6.2.5 Magánkulcs mentése

Szolgáltató, a Regisztrációs Szervezet és Kártyakibocsátó Szervezet az Aláíró magánkulcsát semmilyen formában nem menti, nem tárolja.

6.2.6 Magánkulcs bejuttatása a kriptográfiai modulba

Szolgáltató a hitelesítő központok magánkulcsait a 6.1.1 fejezetben leírtak szerint HSM modulban állítja elő, és azok teljes életciklusuk alatt a HSM modulban maradnak. Amennyiben a magánkulcs visszaállítása rendkívüli üzemi helyzet során szükséges, akkor Szolgáltató a 6.2.4 fejezet szerint végzi a magánkulcsot bejuttatását a kriptográfiai modulba.

Aláíró kulcspárját Szolgáltató megbízásából a Kártyakibocsátó vagy a Regisztrációs Szervezetnek fizikailag védett és biztonságos környezetben, magán az eSZIG elektronikus tároló elemén állítja elő, így annak bejuttatása a kriptográfiai modulba nem szükséges.

6.2.7 Magánkulcs kriptográfiai modulban tárolásának módja

A hitelesítő központok magánkulcsai teljes életciklusuk alatt a 6.2.1 fejezetben leírt HSM modulban kerülnek tárolásra.

Az Aláírók magánkulcsai teljes életciklusuk alatt a 6.2.1 fejezetben leírt eSZIG tároló elemén kerülnek tárolásra.

6.2.8 Magánkulcs aktiválásának módja

A hitelesítő központok magánkulcsainak aktiválását Szolgáltató a HSM modul gyártója által előírt dokumentációja leírtak szerint kell végezze.

Aláíró a magánkulcs aktiválását a számára átadott, PUK és PIN kódokat tartalmazó borítékban levő tájékoztatóban előírtaknak megfelelően kell végezze.

6.2.9 Magánkulcs aktív állapotának megszüntetési módja

Szolgáltatónak biztosítani kell, hogy az aktivált HSM modul jogosulatlan hozzáférés ellen védett legyen. A HSM modul működése során csak az azonosított és feljogosított Kártyakibocsátó Szervezettől érkezett, hiteles tanúsítványkérelmekre kiadott tanúsítványok, visszavonási válaszok és opcionálisan OCSP válaszok aláírására használható. A magánkulcs eltávolításra kerül a HSM modulból, amikor a hitelesítő központ működése megszűnik.

6.2.10 Magánkulcs megsemmisítésének módja

A hitelesítő központok magánkulcsát fizikailag meg kell semmisíteni, amikor használatuk már nem szükséges vagy a kapcsolódó tanúsítvány lejárt vagy visszavonásra került. A magánkulcsot és az aktiválásához szükséges minden adatot olyan módon kell megsemmisíteni, hogy annak végrehajtása után a magánkulcs semmilyen része ne legyen kikövetkezhető vagy levezethető.

Új tanúsítvány igénylése esetén Aláíró magánkulcsa az eSZIG tároló elemén törlésre, illetve felülírásra kerül.

6.2.11 Kriptográfiai modul értékelése

Lásd a 6.2.1 fejezetben.

6.3 Kulcspár gondozás egyéb szempontjai

6.3.1 Nyilvános kulcs archiválása

Szolgáltató köteles minden általa kibocsátott tanúsítvánnyal hitelesített nyilvános kulcsot a tanúsítványba foglalva archiválni és az érvényesség lejártától számított tíz évig megőrizni.

6.3.2 Tanúsítvány érvényességi időszaka és kulcspár felhasználás időtartama

A kulcspár felhasználás időtartama azonos a nyilvános kulcs hitelességét igazoló tanúsítvány érvényességi idejével.

"Főtanúsítványkiadó - Kormányzati Hitelesítés Szolgáltató"	20 év
"Minősített Állampolgári Tanúsítványkiadó"	legfeljebb 15 év
OCSP válaszadó	legfeljebb 30 nap
Aláírói tanúsítvány	legfeljebb 2 év *

*: Az Aláíró tanúsítványának érvényességi ideje két év, ha a kibocsátás időpontjában az eSZIG érvényességéből több mint két év van hátra; ellenkező esetben a tanúsítvány érvényességének vége megegyezik az eSZIG lejárat dátumával.

6.4 Aktivizáló adatok

6.4.1 Aktivizáló adatok előállítása és telepítése

Az eSZIG tároló eleméhez rendelt PUK kódot és Aláíró aláírás-létrehozó adatának (magánkulcsának) használatát engedélyező PIN kódot Szolgáltató megbízásából és nevében a Kártyakibocsátó Szervezetnek fizikailag védett környezetben és biztonságos módon kell előállítania.

6.4.2 Aktivizáló adatok védelme

Az eSZIG tároló eleméhez rendelt PUK és PIN kódot tartalmazó borítékokat a Kártyakibocsátó Szervezetnek fizikailag védett környezetben, az eSZIG-től elkülönítve kell tárolnia. Kártyakibocsátó Szervezet a kódokat csak abból a célból rögzítheti, hogy azok a Regisztrációs Szervezet által az Aláíró számára átadásra kerüljenek.

A Regisztrációs Szervezetnek a kódokat tartalmazó borítékokat személyesen Aláírónak kell átadnia.

Az átvételt követően Aláírónak kell biztosítania a kódok kizárólagos birtoklását és védelmét.

6.4.3 Aktivizáló adatok egyéb szempontjai

Az Aláíró által személyesen átvett PUK és PIN kódot tartalmazó borítékokban levő PIN kód úgynevezett "aktiváló" PIN kód, ami azt jelenti, hogy az aláírás-létrehozó adat (magánkulcs) első használata előtt, az aktiváló PIN kód megadása után kell létrehozni az aláírói hozzáférés jogosultságot biztosító PIN kódot, amellyel a továbbiakban használhatja a magánkulcsot (az eSZIG-et) elektronikus aláírás létrehozására.

A PIN kód sikertelen megadása esetén a PUK kódot kell megadnia a PIN kód cseréjéhez.

A PUK kód hiányában vagy sikertelen megadása esetén a PIN kód cseréjét Aláíró a Regisztrációs Szervezetnél, személyazonosságának igazolásával, személyesen kérheti.

6.5 Informatikai biztonsági óvintézkedések

6.5.1 Informatikai biztonsági műszaki követelmények meghatározása

Az informatikai biztonság műszaki követelményeit a Szolgáltató az {Sz1} ETSI TS 119 401, {Sz2} ETSI TS 119 411-1 és {Sz3} ETSI TS 119 411-2 szabványoknak a minősített szolgáltatások nyújtására vonatkozó, informatikai biztonsági műszaki követelményeiben határozza meg.

Ennek alapján Szolgáltatónak olyan megbízható informatikai rendszert (beleértve a redundáns kiépítést) és technikákat kell kialakítania és üzemeltetnie, melyek biztosítják a Szolgáltató megbízható működését a Szolgáltatások nyújtásához. Ennek ismertetését a Szolgáltató részben a szolgáltatási szabályzatában (HSZSZ-ESZIG), részben a belső biztonsági szabályzataiban írja le.

6.5.2 Informatikai biztonsági értékelés

Szolgáltatónak az informatikai rendszerek biztonsági értékelését az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény rendelkezései szerint kell elvégeznie.

6.6 *Életciklusra vonatkozó műszaki óvintézkedések*

6.6.1 Rendszerfejlesztési óvintézkedések

Szolgáltatónak gondoskodnia kell arról, hogy az általa vagy a nevében végzett valamennyi rendszerfejlesztési projektjében a biztonság követelményeit már a tervezési és követelmény meghatározási fázisban figyelembe vegyék annak érdekében, hogy a biztonság beépüljön az informatikai rendszerekbe.

6.6.2 Biztonságkezelési óvintézkedések

Szolgáltató olyan eszközöket és eljárásokat kell alkalmazzon, melyek garantálják a Szolgáltatásokat megvalósító, megbízható informatikai rendszereinek konfigurációs beállításai, az operációs rendszer beállítások, a hálózati konfigurációs beállítások, továbbá az alkalmazott biztonsági mechanizmusok sértetlenségének és helyes működésének ellenőrzését.

A biztonságkezelési szabályokat a Szolgáltató belső társasági szintű és rendszer szintű információbiztonsági szabályzata tartalmazza.

6.6.3 *Életciklus biztonsági óvintézkedések*

Szolgáltatónak rendszeres időközönként el kell végeznie a Szolgáltatásokat megvalósító, megbízható informatikai rendszereinek konfigurációs beállításai, az operációs rendszer beállítások, a hálózati konfigurációs beállítások, továbbá az alkalmazott biztonsági mechanizmusok sértetlenségének és helyes működésének ellenőrzését.

6.7 *Hálózatbiztonsági óvintézkedések*

A hálózati védelmi intézkedéseket a Szolgáltató belső biztonsági szabályzata "fokozott biztonsági osztály" követelményeinek megfelelően kell megvalósítani, melyek lefedik az {Sz3} ETSI TS 119 411-2 szabvány 6.5.7 fejezetében leírt követelményeket is.

6.8 *Időforrások*

A Szolgáltatások nyújtásához használt megbízható rendszereket rendszeres időközönként, megbízható időforrásokkal (NTP) szinkronizálni kell.

7 TANÚSÍTVÁNY, CRL ÉS OCSP PROFILOK

7.1 Tanúsítvány profil

Szolgáltató által kiadott tanúsítványok megfelelnek az {Sz8} RFC 5280 és az {Sz4} ETSI TS 119 412-1, {Sz5} ETSI TS 119 412-2, {Sz6} ETSI TS 119 412-5 műszaki szabványoknak.

7.1.1 Verziószám

A tanúsítványok verziószáma: V3.

7.1.2 Tanúsítvány kiterjesztések

A tanúsítványokban alkalmazott kiterjesztések mindenben követik az {Sz8} RFC 5280 és az {Sz4} ETSI TS 119 412-1, {Sz5} ETSI TS 119 412-2, {Sz6} ETSI TS 119 412-5 műszaki szabványok előírásait.

7.1.3 Algoritmus azonosítók

A tanúsítványok aláírásához alkalmazott algoritmus azonosítók az alábbiak:
SHA256WithRSAEncryption {iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 11}

7.1.4 Név formák

A név formák leírását és azok értelmezési szabályait a 3.1 fejezet tartalmazza.

7.1.5 Név megszorítások

Szolgáltató a tanúsítványokban név megszorításokat (`NameConstraints`) nem tüntet fel.

7.1.6 Hitelesítési rend objektumazonosító

Szolgáltató a tanúsítványokban feltünteti a hitelesítési rend objektumazonosítóját.

7.1.7 Szabályzati megszorítások kiterjesztés használata

Szolgáltató a tanúsítványban szabályzati megszorításokat (`PolicyConstraints`) nem tüntet fel.

7.1.8 Szabályzat minősítők szintaktikája és szemantikája

A tanúsítványban feltüntetett szabályzat minősítők (`PolicyQualifiers`) és megfelelő szöveg (`UserNotice`) jelzi a tanúsítvány alkalmazhatóságát.

7.1.9 A kritikus hitelesítési rendek (Certificate Policies) kiterjesztés feldolgozása

A tanúsítvány hitelesítési rendek (CertificatePolicies) kiterjesztése nincs kritikusként megjelölve.

7.2 CRL profil

Szolgáltató által kiadott visszavonási listák megfelelnek az {Sz8} RFC 5280 műszaki szabványnak.

7.2.1 Verziószám

A visszavonási listák verziószáma: V2.

7.2.2 CRL és CRL bejegyzés kiterjesztések

A visszavonási lista az alábbi kiterjesztéseket tartalmazza "nem kritikus" megjelöléssel:

`CRLNumber` a visszavonási lista szigorúan növekvő sorszáma

`AuthorityKeyIdentifier` a kibocsátó CA kulcs azonosítója

A visszavonási lista a fentiekén túl más szabványos kiterjesztést is tartalmazhat, azonban ezen kiterjesztések nem lehetnek "kritikus" jelzésűek.

7.3 OCSP profil

Szolgáltató által biztosított OCSP szolgáltatás megfelel az {Sz12} RFC 6960 műszaki szabványnak.

7.3.1 Verziószám

Az OCSP válaszok verziószáma: V1.

7.3.2 OCSP kiterjesztések

Az OCSP válasz az alábbi kiterjesztéseket tartalmazza "nem kritikus" megjelöléssel:

`Nonce` az OCSP kérdésben megadott, visszajátszásos támadások megelőzésére szolgáló véletlenszám (csak akkor, ha a kérdés tartalmazta azt)

`ArchiveCutoff` az időpont, ameddig Szolgáltató a tanúsítvány lejáratát után is biztosítja a visszavonási státuszt

Az OCSP válasz a fentiekén túl más szabványos kiterjesztést is tartalmazhat, azonban ezen kiterjesztések nem lehetnek "kritikus" jelzésűek.

8 MEGFELELŐSÉG VIZSGÁLAT ÉS EGYÉB ÉRTÉKELÉSEK

Jelen hitelesítési rend előírja az összes, a természetes személyek számára kibocsátott minősített tanúsítványokkal kapcsolatos szolgáltatások során teljesíteni szükséges követelményt, melyeket a különösen az alábbi nemzetközi szabványok határoznak meg:

- ETSI TS 119 401: General policy requirements for Trust Service Providers {Sz1}
- ETSI TS 119 411-1: Policy and security requirements for Trust Service Providers issuing certificates {Sz2}
- ETSI TS 119 411-2: Policy and security requirements for Trust Service Providers issuing EU qualified certificates {Sz3}
- ETSI TS 119 412-1: Certificate Profiles; Part 1: Overview and common data structures {Sz4}
- ETSI TS 119 412-2: Certificate Profiles; Part 2: Certificate profiles for certificates issued to natural persons {Sz5}
- ETSI TS 119 412-5: Certificate Profiles; Part 5: QCStatements {Sz6}

8.1 Vizsgálatok gyakorisága és körülményei

A Szolgáltató vizsgálatának gyakorisága és körülményei meg kell feleljen a hatályos jogszabályi előírásoknak.

A 2016. június 30. napjáig terjedő időszakban évente egyszer külső elektronikus aláírási szakértői vizsgálatot kell végezni, a {J4} Ebt., valamint a {J9} 3/2005 IHM rendeletben foglaltak szerint.

2016. július 1. napjával kezdődően, Szolgáltatónak legalább 24 havonta egyszer megfelelőségértékelést kell végeztetnie a {J1} eIDAS 3. cikk 18. bekezdésben meghatározott megfelelőségértékelő szervezettel, a {J1} eIDAS, illetve a {J3} Ebszt. követelményeinek való megfelelés tárgykorben. Szolgáltató köteles az elkészült megfelelőségértékelés jelentést annak kézhezvételétől számított három munkanapon belül benyújtani a Felügyeleti Szervnek.

Az e pont szerint készített első megfelelőségértékelési jelentést a lehető leghamarabb, de legkésőbb 2017. július 1. napjáig be kell nyújtani a Felügyeleti Szervnek.

8.2 Auditor azonosítása és képesítése

A külső rendszervizsgáló által végzett auditokat Szolgáltató olyan, elektronikus aláírási szolgáltatási szakértői névjegyzékben szereplő szakértővel végezteti el, aki független Szolgáltatótól, illetve az ellenőrzött rendszertől, területtől, és szakértelmét biztosítani tudja a PKI és az informatikai biztonság, valamint az ezen területekre vonatkozó technikai, technológiai, jogi, szabályzati ismeretek és auditálási módszertanok vonatkozásában.

A megfelelőségértékelési vizsgálatot Szolgáltató olyan, a 765/2008/EK rendelet 2. cikkének 13. pontjában meghatározott megfelelőségértékelő szervezettel végezteti el, melyet az említett rendelettel összhangban illetékesnek ismernek el a minősített szolgáltató és az általa nyújtott minősített szolgáltatások megfelelőségének értékelésére.

A Szolgáltató tevékenységére és az informatikai biztonságra vonatkozó belső ellenőrzéseket a Szolgáltató belső szervezete végzi, az ott dolgozó biztonsági tisztviselők bevonásával.

8.3 Auditor függetlensége

A megfelelőségértékelő szervezet, annak munkatársai, valamint a külső rendszervizsgáló teljes mértékben függetlenek Szolgáltatótól.

8.4 Audit során vizsgált területek

Az audit az alábbi területeket fedi le:

- szabályzatok és dokumentációk;
- irányítási és ellenőrzési követelmények;
- személyzeti biztonsági követelmények;
- a szolgáltatói kulcspár kezeléséhez kapcsolódó követelmények;
- üzemeltetési és hozzáférési biztonság;
- fizikai és környezeti biztonság;
- folyamatos szolgáltatás biztosítása;
- adatbiztonság és archiválás.

Az audit során megvizsgálásra kerül, hogy Szolgáltató és az általa nyújtott Szolgáltatások megfelelnek:

- hatályos jogszabályoknak és szabványoknak;
- a szolgáltatási szabályzatnak, illetve a hitelesítési rendnek.

8.5 Hiányosságok esetén végrehajtandó tevékenységek

Az üzemszerű ellenőrzések, belső és külső auditok, szakértői elemzések által feltárt hiányosságok, hibás gyakorlatok kezelésére Szolgáltató intézkedési tervet készít. A hiányosságokat késlekedés nélkül orvosolja, az intézkedéseket dokumentálja és ellenőrzi.

A Felügyeleti Szerv (hatóság) által végzett rendszeres helyszíni ellenőrzések során feltárt esetleges hiányosságokat Szolgáltató a hatósággal megállapodott határidőn belül megszünteti a hatályos jogszabályok alapján és a hatóságtól kapott információk és ajánlások figyelembe vételével.

8.6 Eredmény kommunikációja

A belső és külső auditot, szakértői elemzést végző személyek csak a megbízójuknak adhatnak információt a Szolgáltató tevékenységével kapcsolatban. Az audit és az ellenőrzés eredményei a Szolgáltató bizalmas üzleti információi, ezért azokat a társaság titokvédelmi előírásai szerint kell kezelni, azonban a hiányosságok felszámolásáról a felügyelet szervet a következő helyszíni ellenőrzés során tájékoztatni kell. Szolgáltató nem köteles a konkrét hiányosságot nyilvánosságra hozni.

9 EGYÉB ÜZLETI ÉS JOGI KÉRDÉSEK

9.1 Díjak

A díjazással kapcsolatos információkat a HSZSZ-ESZIG szolgáltatási szabályzat tartalmazza.

9.2 Anyagi felelősség

Szolgáltatónak az anyagi felelősség mértékéről, illetve annak korlátairól a szolgáltatási szabályzatban rendelkeznie kell.

9.2.1 Felelősségbiztosítás

Szolgáltatónak felelősségbiztosítással kell rendelkeznie, mely egyaránt kiterjed az elektronikus aláírással, illetve az ezzel ellátott elektronikus dokumentummal szerződésen kívül okozott károkra és szerződésszegéssel okozott károkra, és amely fedezetet biztosít az összes károsultnak okozott kárra, a tanúsítványban jelzett tranzakciós limit értékének legalább ötszörösége.

9.2.2 További követelmények

Nincs kikötés.

9.2.3 Felelősségbiztosítás vagy garancia végfelhasználók számára

Nincs kikötés.

9.3 Üzleti információk bizalmassága

9.3.1 Bizalmasan kezelendő információk köre

Szolgáltatónak a szolgáltatási szabályzatában meg kell adnia a bizalmasan kezelendő információk körét.

9.3.2 Bizalmasnak nem tekintett információk köre

Nincs kikötés.

9.3.3 Bizalmas információk védelmének felelőssége

Szolgáltatónak meg kell védenie a bizalmas információkat. A bizalmas információk védelmét a személyzet megfelelő képzésével, továbbá a munkavállalókkal, szerződéses partnerekkel megkötött szerződésekkel kell érvényre juttatni.

9.4 Személyes adatok védelme

9.4.1 Adatvédelmi terv

Szolgáltató rendelkezik mind társasági szintű adatvédelmi tervvel ({D4}), mind pedig a Szolgáltatásokra vonatkozó adatvédelmi tájékoztatóval, melyek nyilvános dokumentumok, és elérhetők Szolgáltató internetes honlapján. Ezen dokumentumok összhangban vannak a nemzetközi és hazai vonatkozó jogszabályokkal.

Szolgáltató, mint adatkezelő, szerepel a Nemzeti Adatvédelmi és Információszabadság Hivatal Adatvédelmi Nyilvántartásában.

9.4.2 Bizalmasként kezelendő személyes adatok

Szolgáltató csak Aláírótól közvetlenül, annak kifejezett írásos hozzájárulásával gyűjt személyes adatot és csak olyan mértékben, ami a tanúsítvány kiállításához, valamint Aláíró tájékoztatásához, személyazonosságának megállapításához szükséges.

Szolgáltató bizalmasként kezelendő személyes adatnak tekinti:

- Aláíró minden adatát, ha Aláíró nem járult hozzá tanúsítványának közzétételéhez;
- Aláírónak azon adatait, melyek a tanúsítványba nem kerülnek befoglalásra, ha Aláíró írásban hozzájárult tanúsítványának közzétételéhez.

9.4.3 Bizalmasként nem kezelendő személyes adatok

Szolgáltató nem bizalmasként kezelendő személyes adatnak tekinti Aláírónak a tanúsítványba foglalt adatait, amennyiben Aláíró tanúsítványa közzétételéhez írásban hozzájárult.

Továbbá, nem bizalmas adat a tanúsítványhoz kapcsolódó státusz információ, minden tanúsítvány vonatkozásában. A státusz információba beleértendő a tanúsítvány - esetleges - visszavonásának oka és időpontja.

9.4.4 Személyes adatok védelmének felelőssége

Szolgáltató felelős a személyes adatok védelméért.

9.4.5 Hozzájárulás a személyes adatok felhasználásához

Aláírónak a Szolgáltatási Szerződés aláírásával hozzá kell járulnia a tanúsítvány kiállításához és a szerződés megkötéséhez szükséges adatok Szolgáltató által történő nyilvántartásba vételéhez, kezeléséhez és tárolásához.

Aláíró választása szerint hozzájárulhat vagy megtilthatja tanúsítványának nyilvános közzétételét.

9.4.6 Felfedés hatósági vagy polgári peres eljárás keretében

A Szolgáltató bűncselekmények felderítése vagy megelőzés céljából, illetve nemzetbiztonsági érdekből - az adatigénylésre meghatározott jogszabályi feltételek teljesülése esetén - a nyomozó

hatóságnak és a nemzetbiztonsági szolgálatoknak haladéktalanul és egyéb feltételek nélkül feltárja a jogszabályban meghatározott bizalmas információkat. Szolgáltató rögzíti az adatátadás tényét, de arról nem tájékoztatja érintett Aláíró.

Szolgáltató a tanúsítvány érvényességét érintő polgári peres, illetve nem peres eljárás során - az érintettség igazolása esetén - az ellenérdekű peres félnek vagy képviselőjének, valamint a megkereső bíróságnak feltárhatja a jogszabályban meghatározott bizalmas információkat. Szolgáltató rögzíti az adatátadás tényét, és arról tájékoztatja érintett Aláíró.

9.4.7 Egyéb felfedést eredményező körülmények

Szolgáltató a szolgáltatási tevékenység, illetve a Szolgáltatások nyújtásának megszüntetése esetén Aláíró adatait a jogszabályi kötelezettségeire tekintettel átadja harmadik félnek.

9.5 Szellemi tulajdonjogok

A Szolgáltató által Aláíró részére kibocsátott tanúsítvány és az ahhoz tartozó kulcspár tulajdonosa az Aláíró. Szolgáltató a tanúsítványt a kikötéseiben és feltételeiben ismertetett esetekben és módon a tanúsítványt közzéteheti, sokszorosíthatja, visszavonhatja és egyéb módon is kezelheti. A végfelhasználói tanúsítványban szereplő megkülönböztető név használatára Aláíró jogosult.

A szolgáltatói tanúsítványok a Szolgáltató tulajdonát képezik. A visszavonási információk a Szolgáltató tulajdonát képezik. A Szolgáltató szabályzatai, szerződéses feltételei a Szolgáltató tulajdonát képezik.

9.6 Tevékenységért viselt felelősség és helytállás

9.6.1 Szolgáltató felelőssége és helytállása

Szolgáltató felel a jelen hitelesítési rendben és a vonatkozó szolgáltatási szabályzatban, valamint az Aláíróval megkötött Szolgáltatási Szerződésben megfogalmazott valamennyi kötelezettség maradéktalan betartásáért, még akkor is, ha a Szolgáltatások nyújtásához kapcsolódó egyes feladatokat a Közreműködő Felek vagy egyéb alvállalkozók végzik.

9.6.2 A regisztrációs szervezet felelőssége és helytállása

9.6.2.1 Regisztrációs Szervezet felelőssége és helytállása

Regisztrációs Szervezet betartja a rá vonatkozó jogszabályokban, illetve a Szolgáltató szabályzataiban foglalt előírásokat.

Regisztrációs Szervezet felelőssége a tanúsítvány kiadásával kapcsolatban:

- A tanúsítvány kibocsátását kérő személy teljes körű és közérthető tájékoztatása a 4.1.2 fejezetben meghatározottakról;
- az igénylő azonosítása a 3.2 fejezetben leírt eljárással;
- az igénylő aláírói tanúsítványra jogosultságának elbírálása;
- a tanúsítványba foglalandó adatok egyeztetése és ellenőrzése közhiteles nyilvántartások

alapján;

- a regisztrációhoz és a Szolgáltatási Szerződés megkötéséhez szükséges, egyeztetett és ellenőrzött adatok rögzítése az erre szolgáló informatikai rendszerben;
- közreműködés a Szolgáltatási Szerződés megkötésében;
- PUK és PIN kódokat, továbbá a visszavonási jelszót tartalmazó borítékok átadása személyesen Aláírónak, arról az átvételi elismervény felvétele;
- kezdeményezni azt, hogy a Kártyakibocsátó Szervezet az eSZIG tároló elemét Aláíró részére megszemélyesítse;
- közreműködni abban, hogy Szolgáltató által Aláíró számára kibocsátott tanúsítvány az eSZIG-re felírásra kerüljön;
- annak biztosítása, hogy az eSZIG Aláíró számára személyes átadásra vagy kézbesítésre kerüljön, valamint hogy Aláíró a megfelelő eSZIG-et (a sajátját) kapja kézhez.

Regisztrációs Szervezet felelőssége a tanúsítványok visszavonásával kapcsolatban:

- intézkedni arról, hogy Aláíró kérésére a visszavonási igény rögzítésre kerüljön és a visszavonást kezdeményezze a Szolgáltató felé;
- intézkedni arról, hogy a bármilyen okból (eltulajdonítás, megsemmisülés, elvesztés, adatváltozás, elhalálozás miatt) érvénytelenített eSZIG-hez tartozó tanúsítvány visszavonását kezdeményezze a Szolgáltató felé.

9.6.2.2 Kártyakibocsátó Szervezet felelőssége és helytállása

Szolgáltató a Kártyakibocsátó Szervezettel megkötött együttműködési megállapodásban meg kell követelje a hitelesítési rend és a vonatkozó szolgáltatás szabályzat előírásainak maradéktalan betartását.

Kártyakibocsátó Szervezet felelőssége:

- az eSZIG tároló elemén, mint elektronikus aláírást létrehozó eszközön a Felügyeleti Szerv vonatkozó határozatának megfelelő algoritmusú és paraméterű, kulcspárok generálása szigorúan védett és biztonságos környezetben és módon, a BALE tanúsítási jelentésében meghatározott előírások betartásával;
- aktivizáló adatok és visszavonási jelszavak előállítása és tárolása biztonságos módon, a kártyáktól elkülönítve;
- az eSZIG-nek, mint elektronikus aláírást létrehozó eszköznek a megszemélyesítése, úgy, hogy az Aláíró adataival megfelelően kitöltött és Aláíró eSZIG-jének tároló elemén előállított magánkulcshoz tartozó nyilvános kulcsot tartalmazó tanúsítványkérelem kerüljön összeállításra;
- a tanúsítványkérelmek hitelesítése szervezeti elektronikus aláírással és a kérelmek eljuttatása Szolgáltató részére;
- Szolgáltató által kibocsátott tanúsítvány felírása az eSZIG tároló elemére;
- az eSZIG biztonságos tárolása annak kézbesítéséig;
- annak biztosítása, hogy az eSZIG - a Regisztrációs Szervezet, illetve a Postai Szolgáltató által – Aláíró számára átadásra kerüljön és Aláíró a megfelelő eSZIG-et kapja kézhez;
- annak biztosítása - a Regisztrációs Szervezettel együttműködve -, hogy az eSZIG aktiválását csak Aláíró legyen képes elvégezni;
- a tanúsítvány visszavonási kérelmek hitelesítése szervezeti elektronikus aláírással és a kérelmek eljuttatása Szolgáltató részére.

9.6.3 Aláíró felelőssége és helytállása

Aláíró felelőssége

- Aláíró felelős a regisztráció során megadott adatai valódiságáért, pontosságáért és érvényességéért.
- Aláíró felelős a tanúsítványban szereplő adatok ellenőrzéséért.
- Aláíró felelős azért, hogy a tanúsítványt érintő összes adatának megváltozását haladéktalanul bejelentse, beleértve mindazon adataiban bekövetkezett változásokat is, melyeket a regisztrációs eljárás és a Szolgáltatási Szerződés megkötése során megadott.
- Aláíró felelős az eSZIG-nek mint biztonságos aláírás-létrehozó eszköznek, valamint a kapcsolódó magánkulcsnak a rendeltetésszerű felhasználásáért, a szabályzatoknak és a BALE tanúsítási jelentésében előírtaknak megfelelően.
- Aláíró felelős a magánkulcsnak, az aktivizáló kódjainak és a visszavonási jelszónak a biztonságos kezeléséért.
- Aláíró felelős azért, hogy a magánkulcsot és a kapcsolódó tanúsítványt csak a tanúsítvány érvényességi időtartamán belül használja, a tanúsítvány visszavonása esetén azok használatát haladéktalanul és végérvényesen beszüntesse.
- Aláíró felelős Szolgáltatót haladéktalanul értesíteni és teljes körűen tájékoztatni vitás ügyekben.
- Aláíró felelős a Szolgáltatási Szerződésben és a {D1} Általános Szerződési Feltételekben meghatározott kötelezettségei betartásáért.

9.6.4 Érintett Felek felelőssége és helytállása

Az Érintett Felek a saját belátásuk és/vagy szabályzataik szerint dönthetnek az egyes tanúsítványok elfogadásáról és a felhasználás módjáról. A tanúsítvány érvényességének elbírálása során az Érintett Félnek megfelelő körültekintéssel kell eljárnia, ezért különös tekintettel javasolt:

- a szolgáltatási szabályzatban foglalt követelmények és előírások betartása;
- megbízható informatikai környezet és alkalmazások használata;
- a tanúsítvány felhasználására vonatkozó valamennyi korlátozás figyelembe vétele, amely a tanúsítványban vagy a szolgáltatási szabályzatban szerepel.

9.6.5 Egyéb felek felelőssége és helytállása

Nincs kikötés.

9.7 Helytállás érvénytelenségi köre

A helytállás érvénytelenségi körét a szolgáltatási szabályzatban meg kell határozni.

9.8 Felelősség korlátozása

Szolgáltató korlátozhatja a kártérítési felelősségét:

- a tanúsítvánnyal egy alkalommal vállalható kötelezettség mértékében (tranzakciós limit);
- összességében az összes tanúsítvánnyal és káreseménnyel kapcsolatban.

9.9 Kártérítések

A kártérítésekről a szolgáltatási szabályzatban kell rendelkezni.

9.10 Hatályosság és megszűnés

9.10.1 Hatályosság

Időbeli hatály

A hitelesítési rend egy adott verziójának időbeli hatálya a címlapon feltüntetett hatálybalépés dátumával kezdődik és határozatlan időre szól. Az időbeli hatály megszűnik a hitelesítési rend újabb verziójának hatályba lépésével vagy a Szolgáltatások befejezésekor.

Tárgyi hatály

A hitelesítési rend tárgyi hatálya kiterjed a Szolgáltatások nyújtására és igénybe vételére.

Személyi hatály

A hitelesítési rend személyi hatálya kiterjed Szolgáltatónak illetve a Közreműködő Feleknek a Szolgáltatások nyújtásában közreműködő munkatársaira és az Aláírókra.

9.10.2 Megszűnés

A hitelesítési rend a Szolgáltató szolgáltatási tevékenységének befejezésével tekintendő megszűntnek.

9.10.3 Megszűnés után is hatályban maradó rendelkezések

A megszűnés után is hatályban maradó rendelkezéseket a szolgáltatási szabályzatban meg kell határozni.

9.11 Egyéni hirdetmények és kommunikáció a résztvevőkkel

A szolgáltatási szabályzatban rendelkezni kell a felek és résztvevők között kommunikáció joghatást kiváltó módjairól.

9.12 Módosítások

9.12.1 Módosítás eljárása

A hitelesítési rend módosítása az 1.5.3 és 1.5.4 fejezetekben leírt szabályok szerint történik. A hitelesítési rend módosulását a verziószám megfelelő változása jelzi.

9.12.2 Értesítés módszere és időtartama

A Szolgáltatások jelentős vagy lényeges változása esetén Szolgáltatónak internetes honlapján közleményt kell közzétennie, a hatályba lépést megelőzően kellő időben ahhoz, hogy az érintett a

felek a változásokra felkészülhessenek.

9.12.3 *OID megváltozását előidéző körülmények*

A hitelesítési rend új verziójával az OID verziószámot jelentő része megfelelően változik.

9.13 *Vitás kérdések rendezése*

A szolgáltatási szabályzat tartalmazza.

9.14 *Irányadó jog*

Szolgáltató szerződéseire, szabályzataira és azok teljesítésére a magyar jog az irányadó és azokat a magyar jog szerint kell értelmezni.

9.15 *Hatályos jognak megfelelés*

Szolgáltató tevékenységét a mindenkor hatályos Európai Unió, illetve magyar jogszabályoknak megfelelően köteles végezni.

9.16 *Vegyes rendelkezések*

9.16.1 *Teljességi záradék*

Nincs kikötés.

9.16.2 *Átruházás*

Nincs kikötés.

9.16.3 *Részleges érvénytelenség*

A jelen hitelesítési rend egyes rendelkezéseinek tetszőleges okból történő érvénytelenné válása esetén a többi rendelkezés változatlan formában érvényben marad.

9.16.4 *Igényérvényesítés*

Szolgáltató kártérítésre, az ügyvédi díjak megfizetésére tarthat igényt a partnerei által okozott károk, veszteségek, költségek megtérítése érdekében. Amennyiben Szolgáltató egy konkrét esetben nem él kártérítési igényével, az nem jelenti azt, hogy a jövőben hasonló esetben a hitelesítési rend más rendelkezésének megsértése esetén is lemondana a kártérítési igény érvényesítéséről.

9.16.5 *Vis maior*

A szolgáltatási szabályzat tartalmazza.

9.17 *Egyéb rendelkezések*

9.17.1 Hozzáférhetőség a fogyatékossgal élő személyek számára

A Szolgáltatásokat és a Szolgáltatások során alkalmazott végfelhasználó termékeket hozzáférhetővé kell tenni a fogyatékossgal élő személyek számára, amennyiben az lehetséges.